EXHIBIT B-1

Committee on Oversight and Government Reform
U.S. House of Representatives
114th Congress

The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation

Majority Staff Report

Hon. Jason Chaffetz, Chairman
Committee on Oversight and Government Reform

Hon. Mark Meadows, Chairman
Subcommittee on Government Operations

Hon. Will Hurd, Chairman
Subcommittee on Information Technology

September 7, 2016

www.oversight.house.gov

A Letter from the Chairman

September 7, 2016

To Federal Chief Information Officers:

The advent of the information age presents a paradigm shift about how our federal institutions collect, store, distribute, and protect information. The data breach at the U.S. Office of Personnel Management (OPM) is a defining moment, and it is up to you—the community of federal chief information officers—to determine how the country will respond.

The effectiveness of our country's response depends on your answer to this question: Can you as the CIO be trusted with highly personal, highly sensitive data on millions of Americans? Federal CIOs possess expertise and technical knowledge that support the mission-related activities of their agency. As Departmental heads focus on managing the bureaucracy of the executive branch, substantive challenges of their agencies' mission, and Congress, CIOs play a critical role in keeping technology working for Americans, and in furtherance of the agencies' mission.

Federal CIOs matter. In fact, your work has never been more important, and the margin for error has never been smaller.

As we continue to confront the ongoing challenges of modernizing antiquated systems, CIOs must remain constantly vigilant to protect the information of hundreds of millions of Americans in an environment where a single vulnerability is all a sophisticated actor needs to steal information, identities, and profoundly damage our national security.

The mission of our Committee is to ensure the efficiency, effectiveness, and accountability of the federal government and its agencies. We have a constitutional duty to provide meaningful oversight of the executive branch and to recommend reforms that are informed by our investigative findings. Taxpayers also rely on the Committee to bring a measure of accountability and transparency in cases where there is evidence of misconduct.

That is why I am releasing this report to the American public. For those whose personal information was compromised, I hope this report provides some answers on the how and why. Most of all, however, it is my hope that the findings and recommendations contained herein will inform and motivate current and future CIOs and agency heads so we – as a government – can be smart about the way we acquire, deploy, maintain, and monitor our information technology. The OPM data breach and the resulting generational national security consequences cannot happen again. It is up leaders like you and Congress to ensure it does not happen again.

Sincerely,

Jason Chaffetz
Chairman

The Damage Done

"This is crown jewels material . . . a gold mine for a foreign intelligence service."

"This is not the end of American human intelligence, but it's a significant blow."[*]

— Joel Brenner, former NSA Senior Counsel

"We cannot undo this damage. What is done is done and it will take decades to fix."[†]

— John Schindler, former NSA officer

"[The SF-86] gives you any kind of information that might be a threat to [the employee's] security clearance."[‡]

— Jeff Neal, former DHS official

"My SF-86 lists every place I've ever lived since I was 18, every foreign travel I've ever taken, all of my family, their addresses. So it's not just my identity that's affected. I've got siblings. I've got five kids. All of that is in there."[§]

— James Comey, Director of the FBI

"[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."[**]

— Michael Hayden, former Director of the CIA

[*] David Perera & Joseph Marks, *Newly Disclosed Hack Got "Crown Jewels,"* POLITICO, June 12, 2015, available at: http://www.politico.com/story/2015/06/hackers-federal-employees-security-background-checks-118954.

[†] *Ex-NSA Officer: OPM Hack is Serious Breach of Worker Trust*, NPR, June 13, 2015, available at: http://www.npr.org/2015/06/13/414149626/ex-nsa-officer-opm-hack-is-serious-breach-of-worker-trust.

[‡] Id.

[§] Maggie Ybarra, *James Comey, FBI Chief, Says His Own Info was Hacked in OPM Breach; It was "Enormous"*, WASH. TIMES, July 9, 2015, available at: http://www.washingtontimes.com/news/2015/jul/9/james-comey-fbi-chief-says-his-own-info-was-hacked.

[**] Dan Verton, *Impact of OPM Breach Could Last More Than 40 Years*, FEDSCOOP.COM, July 12, 2015, available at: http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community.

Executive Summary

The government of the United States of America has never before been more vulnerable to cyberattacks. No agency appears safe. In recent data breaches, hackers took information from the United States Postal Service; the State Department; the Nuclear Regulatory Commission; the Internal Revenue Service; and even the White House.

None of these data breaches though compare to the data breaches at the U.S. Office of Personnel Management (OPM). **In what appears to be a coordinated campaign to collect information on government employees, attackers exfiltrated personnel files of 4.2 million former and current government employees and security clearance background investigation information on 21.5 million individuals.**[1] Additionally, fingerprint data of 5.6 million of these individuals was stolen.

The loss of personally identifiable information (PII) is deeply troubling and citizens deserve greater protection from their government. Further, the damage done by the loss of the background investigation information and fingerprint data will harm counterintelligence efforts for at least a generation to come.

<u>The Significance of What the Attackers Stole</u>. Certain individuals apply for a security clearance to gain access to our country's most sensitive national security secrets. These individuals are required to complete Standard Form 86 or "SF-86" and undergo a background investigation. Many applicants are obvious targets by adversaries for intelligence purposes by virtue of their holding some of the most sensitive positions in our government, including anyone accessing classified information and anyone employed in a "national security sensitive position." This encompasses a wide-range of federal employees and contractors at all federal agencies, including the U.S. Department of Defense and throughout the Intelligence Community.

Background investigations conducted on these individuals are designed to identify the type of information that could be used to coerce an individual to betray their country. Therefore, applicants are required to provide a wealth of information about their past activities and lifestyle. For example, applicants are required to provide extensive financial information, as well as employment history and home addresses for the past ten years. Applicants are also required to provide the names of any relatives, including step-siblings or half-siblings, and their home addresses.

The SF-86 also requests disclosure of some of the most intimate and potentially embarrassing aspects of a person's life, including whether the applicant:

[1] There is some overlap between the 4.2 million individuals impacted by the personnel records breach and the 21.5 million individuals impacted by the background investigation breach. Of the 4.2 million individuals impacted by the personnel records breach, 3.6 million on these individuals also had their background investigation data stolen. *See* Letter from Jason Levine, Dir. Congressional, Legislative & Intergov't Affairs, U.S. Office of Personnel Mgmt. to Jason Chaffetz, Chairman, H. Comm. on Oversight & Gov't Reform (Aug. 21, 2015). The aggregate number of individuals impacted by this breach totals 22.1 million.

- "consult[ed] with a health care professional regarding an emotional or mental health condition;"
- "illegally used any drugs or controlled substances;"
- abused alcohol resulting in "a negative impact on your work performance or personal relationships, your finances, or result in intervention by law enforcement/public safety personnel;" and
- "experienced financial problems due to gambling."

In short, the SF-86 asks individuals to turn over their most personal details; information that in the wrong hands could be used for espionage purposes.

The intelligence and counterintelligence value of the stolen background investigation information for a foreign nation cannot be overstated, nor will it ever be fully known. The Director of the Federal Bureau of Investigation (FBI) James Comey described the data breach as a "very big deal from a national security perspective and from a counterintelligence perspective. It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government."[2]

Nor is there any way to remedy the problem now that the information is in the hands of our adversaries. Former Central Intelligence Agency (CIA) Director Michael Hayden warned he does not "think there is recovery from what was lost" and "it remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it."[3]

<u>How the Breach Happened</u>. Despite this high value information maintained by OPM, the agency failed to prioritize cybersecurity and adequately secure high value data. The OPM Inspector General (IG) warned since at least 2005 that the information maintained by OPM was vulnerable to hackers. In 2014, the IG upgraded issues surrounding information security governance at OPM from a "material weakness" to a "significant deficiency." But fundamental aspects of OPM's information security posture, such as the absence of an effective managerial structure to implement reliable IT security policies, remained a "significant deficiency" or worse since 2007.[4] Indeed, even after the data breach as of November 2015, the OPM IG continued to report that "OPM continues to struggle to meet many FISMA requirements" and with "overall lack of compliance that seems to permeate the agency's IT security program."[5]

[2] Ellen Nakashima, *Hacks of OPM databases compromised 22.1 million people, federal authorities say*, WASH. POST, July 9, 2015, available at: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[3] Dan Verton, *Impact of OPM Breach Could Last More Than 40 Years*, FedScoop.com (July 12, 2015) available at: http://fedscoop.com/opm-losses-a-40-year-problem-for-intelligence-community.

[4] Office of Inspector Gen., U.S. Office of Pers. Mgmt, No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[5] Office of Inspector Gen., U.S. Office of Pers. Mgmt., No. 4A-CI-00-15-011, *Final Audit Report, Federal Information Security Modernization Act Audit FY 2015* 5 (Nov. 10, 2015) available at: https://www.opm.gov/our-inspector-general/reports/2015/federal-information-security-modernization-act-audit-fy-2015-final-audit-report-4a-ci-00-15-011.pdf [hereinafter *FY15 FISMA Audit*].

The agency also failed to implement the Office of Management and Budget's (OMB) longstanding requirement to use multi-factor authentication for employees and contractors who log on to the network. In a 2015 OMB report on IT security, OPM was identified at the end of fiscal year 2014 as one of several agencies with the "weakest authentication profile[s]" and only having one percent of user accounts requiring personal identity verification (PIV) cards for access.[6] The agency also allowed key IT systems, which were later compromised, to operate without a security assessment and valid Authority to Operate (ATO). In 2014, the IG called the increasing number of OPM IT systems operating without a valid ATO "alarming."[7]

The lax state of OPM's information security left the agency's information systems exposed for any experienced hacker to infiltrate and compromise. On March 20, 2014, the U.S. Department of Homeland Security's (DHS) United States Computer Emergency Response Team (US-CERT) notified OPM's Computer Incident Response Team (CIRT) that a third party had reported data exfiltration from OPM's network. In an effort to better understand the threat posed by the hacker, OPM monitored the adversary's movements over a two-month period. **The agency's senior leadership failed to fully comprehend the extent of the compromise, allowing the hackers to remove manuals and other sensitive materials that essentially provided a roadmap to the OPM IT environment and key users for potential compromise.**

While OPM monitored the first hacker (for convenience here we will refer to this actor as Hacker X1), on May 7, 2014 another hacker posed as an employee of an OPM contractor performing background investigations, KeyPoint (which we can call Hacker X2). Hacker X2 used the contractor's OPM credentials to log into the OPM system, install malware, and create a backdoor to the network.

As the agency monitored Hacker X1's movements throughout the network, it noticed Hacker X1 was getting dangerously close to the security clearance background information. OPM, in conjunction with DHS, developed a plan to kick Hacker X1 out of the system. It termed this remediation "the Big Bang." The agency was confident the planned remediation effort in late May 2014 eliminated Hacker X1's foothold on their systems. But Hacker X2, who had successfully established a foothold on OPM's systems and had not been detected due to gaps in OPM's IT security posture, remained in OPM's system post-Big Bang.

<u>The Exfiltration of the Security Clearance Files Could Have Been Prevented</u>. After the May 27 Big Bang, Hacker X2 moved around OPM's system until they began exfiltrating data in July 2014. As OPM's Director of IT Security Operations Jeff Wagner explained, the KeyPoint credential was used for the initial attack vector and then the attacker used various tactics to obtain domain administrator credentials to ultimately perform operations and maintain persistence from malware. Beginning in July through August 2014, the Hacker X2 exfiltrated the security clearance background investigation files. Then in December 2014, personnel records were exfiltrated, and in early 2015, fingerprint data was exfiltrated.

[6] Office of Mgmt. & Budget, Exec. Office of the President, *FY 2014 Annual Report to Congress: Federal Information Security Management Act* at 23, 20 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.

[7] U.S. Office of Personnel Mgmt. Office of the Inspector General, *Federal Information Security Management Act Audit FY 2014* at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

Had OPM implemented basic, required security controls and more expeditiously deployed cutting edge security tools when they first learned hackers were targeting such sensitive data, they could have significantly delayed, potentially prevented, or significantly mitigated the theft. Testimony from DHS made clear OPM's implementation of two-factor authentication for remote logons in early 2015, which had long been required of federal agencies, would have "precluded continued access by the intruder into the OPM network." Further, if OPM had fully deployed in a preventative mode available security tools and had sufficient visibility to fully monitor their network in the summer of 2014, they might have detected and stopped Hacker X2 before they had a chance to exfiltrate the security clearance background investigation files. **Importantly, the damage also could have been mitigated if the security of the sensitive data in OPM's critical IT systems had been prioritized and secured.**

The exact details on how and when the attackers (X1, X2) gained entry and established a persistent presence in OPM's network are not entirely clear. This is in large part due to sloppy cyber hygiene and inadequate security technologies that left OPM with reduced visibility into the traffic on its systems.

The data breach by Hacker X1 in 2014 should have sounded a high level multi-agency national security alarm that a sophisticated, persistent actor was seeking to access OPM's highest-value data. It was not until April 15, 2015 that OPM identified the first indicator its systems were compromised by Hacker X2. From April 16, 2015 through May 2015 (during the primary incident response period), security tools from an outside contractor, Cylance Inc., consistently detected key malicious code and other threats to OPM. While these types of security tools were generally available to OPM, the agency did not choose to deploy a preventative technology until *after* the agency was severely compromised and until *after* the agency's most sensitive information was lost to nefarious actors.

Notably, OPM's Director of IT Security Operations, Jeff Wagner, recommended deploying Cylance's preventative technology to insulate OPM's enterprise from additional attacks after the initial attack by Hacker X1 in March 2014. The Committee obtained documents and testimony proving OPM's information security posture was undermined by a woefully unsecure IT environment, internal politics and bureaucracy, and misplaced priorities related to the deployment of security tools that slowed vital security decisions. **Swifter action by OPM to harden the defenses of its IT architecture could have prevented or mitigated the damage that OPM's systems incurred.**

While OPM continued its incident response efforts throughout April 2015, another outside contractor named CyTech Services, provided forensic support after conducting an onsite demonstration of its technology "CyFIR." While OPM and CyTech provide differing accounts of the role of CyFIR in detecting unknown malware on OPM's systems, it is clear CyTech detected malware and assisted for at least two week in the response to the 2015 data breaches. To date, CyTech has not been compensated for any of its work. The Anti-Deficiency Act (ADA) prohibits a federal agency from accepting voluntary services without payment and without obtaining an agreement in writing that the contractor will never seek payment. In this case, there was no such agreement. Most concerning, the agency destroyed 11,035 files and directories located on CyTech's device prior to returning the device to its owner while a request from the

Committee for this information was pending. All of those files were material to the Committee's investigation, responsive to the Committee's subpoena requests for information and documents, and subject to a preservation order by the Committee.

OPM Misled Congress and the Public to Diminish the Damage. As the agency assessed the damage caused by the hackers, OPM downplayed the fallout. **OPM failed to proactively announce the 2014 breach to the public, and claimed the two cyberattacks were not connected. The 2014 and 2015 incidents, however, appear to be connected and possibly coordinated.** The first confirmed adversarial activity for both incidents came within a two-month span in November and December 2013. The hack discovered in March 2014 by Hacker X1 appeared to move through the system looking for security clearance background investigation data and was removed when they got too close. Hacker X1 did, however, exfiltrate OPM's manuals and other sensitive materials, which would be useful for targeting background information data systems. Hacker X1 was cleared from the system in May 2014 during the Big Bang exercise. Within three months, Hacker X2 finished targeting and stealing OPM's background investigations data (by early August 2014). Hacker X2 later stole personnel records (in December 2014) and fingerprint data (in March 2015). **The two attackers shared the same target, conducted their attacks in a similarly sophisticated manner, and struck with similar timing.** Further, the manuals exfiltrated by Hacker X1 likely aided Hacker X2 in navigating the OPM environment.

The Committee's year-long investigation to understand *how* the attackers perpetrated their intrusion, movements, and ultimately the exfiltration of data began with hearings, wherein then-OPM Chief Information Officer (CIO) Donna Seymour made a series of false and misleading statements under oath regarding the agency's response to the incidents announced in 2015. Seymour testified that OPM purchased CyTech licenses, but OPM did not make any purchases from CyTech. She also testified that CyTech's CyFIR tool was installed in a quarantine environment for the demonstration, but this tool was running on a live environment at OPM when it identified malware on April 22, 2015.

Seymour also misled the public about the significance of the data stolen in the 2014 attack. She testified on April 22, 2015 that "our antiquated technologies may have helped us a little bit."[8] Two months later, on June 24, 2015, she testified that the stolen manuals that were a roadmap to OPM's systems were merely "outdated security documents."[9]

The Bottom Line. The longstanding failure of OPM's leadership to implement basic cyber hygiene, such as maintaining current authorities to operate and employing strong multi-factor authentication, despite years of warnings from the Inspector General, represents a failure of culture and leadership, not technology. As OPM discovered in April 2015, tools were available that could have prevented the breaches, but OPM failed to leverage those tools to mitigate the agency's extensive vulnerabilities.

[8] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't. Reform*, 114th Cong. (Apr. 22, 2015) [hereinafter *Enhancing Cybersecurity Hearing*] (statement of Donna Seymour, Chief Info. Officer of the U.S. Office of Pers. Mgmt.).

[9] *OPM Data Breach: Part II: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 69 (June 24, 2015) (hereinafter *Hearing on OPM Data Breach: Part II*) (statement of Donna Seymour, Chief Info. Officer of the U.S. Office of Pers. Mgmt.).

As a result, tens of millions of federal employees and their families paid the price. Indeed, the damage done to the Intelligence Community will never be truly known. Due to the data breach at OPM, adversaries are in possession of some of the most intimate and embarrassing details of the lives of individuals who our country trusts to protect our national security and its secrets.

This report documents how the government allowed this unthinkable event to happen and makes recommendations in an attempt to ensure this never happens again.

The Committee remains hopeful that OPM, under the new leadership of Acting Director Beth Cobert, is in the process of remedying decades of mismanagement.

Table of Contents

A Letter from the Chairman ii

The Damage Done iii

Executive Summary v

Table of Contents 1

Timeline of Key Events 5

Findings 14

Recommendations 20

Table of Names 28

Chapter 1: OPM's IT Security Record Preceding Breaches 30

The Rise of Advanced Persistent Threat Hacking 30

Federal Contractors Holding Sensitive Federal Employee Information Targeted and Attacked 31

Federal Initiatives to Increase Information Security in Response to Increasing Attacks 34

OPM Failed to Recognize the Threat and Implement Effective IT Security Measures When It Mattered 35

OPM's Cybersecurity Spending Consistently Trailed Other Federal Agencies 36

OPM Attempts to Balance IT Security with Competing Priorities 37

The Katherine Archuleta and Donna Seymour Era 42

OPM Failed to Prioritize the Security of Key Data and Systems 47

Chapter 2: The First Alarm Bell – Attackers Discovered in 2014 Target Background Information Data and Exfiltrate System-Related Data 51

Discovery & Incident Response for Attackers Discovered in 2014 52

Monitoring the Adversary and the May 2014 "Big Bang" to Expel Attackers Discovered in 2014 55

During the 2014 Incident Response Period the Exfiltration of PIPS-related Information Made Clear the Attackers' Target was Background Investigation Data Held in PIPS 62

Tactics Techniques & Procedures (TTPs) of Attackers Discovered in 2014: Hikit Malware and SMB Protocol 67

OPM's Network Logging Capabilities Limited Investigating the "How" and "How Long" for Attackers Discovered in 2014 71

Chapter 3: OPM Attempts to Mitigate the Security Gaps Identified in 2014 While Iron Man and Captain America Go to Work (May 2014 – April 2015) 75

OPM's IT Security Posture and Mitigation Efforts After the May 2014 "Big Bang" 75

Key 2014 US-CERT Recommendations Highlighted OPM IT Security Vulnerabilities 77

OPM Efforts to Buy Security Tools to Secure the Legacy Network and Rebuild OPM's "Very Insecure, Insecurely Architected Network" 79

OPM Missed Key Developments 81

In April 2015, OPM Realized They Were Under Attack – Again 83

Captain America: The First Indicator that Led to the 2015 Discovery of the Background Investigation Data Breach 84
The Avengers: Anatomy of the Data Breach Discovered in 2015 85
Chapter 4: The Role of Cylance Inc. 91
OPM's "Cyber Climate" During Cylance Product Demonstrations 91
Overview of the Cylance Cyber Tools 93
April 15-16, 2015: The First 24 Hours 94
April 17, 2015: US-CERT Confirms PlugX 98
April 17, 2015: CylanceProtect Deployed 100
April 18, 2015: Protect Lights Up Like a Christmas Tree 102
April 19, 2015: Severity of the Situation Becomes Clear 103
April 20-23, 2015 – More Key Trojans Identified; OIG First Notified. 108
April 24-25, 2015 – OPM Upgrades Protect to Auto-Quarantine Mode. 110
April 26 – April 30, 2015: First Signs of Lost Background Materials 113
The Decision to Purchase CylanceProtect 116
Political Challenges on the Desktop 116
Counterpoint – Lack of FedRAMP Compliance 119
OPM Purchases Protect After Nearly Losing Access to It 121
Chapter 5: The CyTech Story 125
CyTech Is a Small Business Contractor with Significant Cyber Tool Capabilities 126
CyTech Was Invited to Conduct a Demo at OPM 127
Prior to the April 21, 2015 CyFIR Demonstration at OPM 128
The April 21, 2015 – April 22, 2015 CyFIR Demonstration at OPM 128
The CyTech Demo Turned into Incident Response and Forensic Support 135
CyTech Provided Onsite Incident Response and Forensic Support From April 23 to May 1, 2015 135
CyFIR Was Deployed on the OPM Network beginning in April 2015 and Remained on OPM's Network through August 2015 138
The *Wall Street Journal* Reports on CyTech's Role in the OPM Incident on June 10, 2015 141
CyTech Coordinated with OPM Prior to the June 10, 2015 Story 142
OPM and CyTech Respond to the Article 143
OPM Description of CyTech's Role Was Misleading 146
Archuleta and Seymour Provided Misleading Testimony to Committee 146
Data on CyTech's CyFIR Appliance Collected During the 2015 Incident Response Period was Deleted 148
OPM Retained CyTech's CyFIR Appliance Through August 2015 149
Before Returning the CyFIR Appliance OPM Deleted Key Data. 149
OPM "Sanitized" the CyFIR Appliance 151
OPM Violated the Anti-Deficiency Act 152
The ADA's prohibition on accepting voluntary services 152
The "gratuitous" services exception 152

The "emergencies" exception 153

The ADA applied to the OPM and CyTech Situation 153

CyTech expected to be paid 154

Chapter 6: Connections Between the 2014 and 2015 Intrusions 157

One Group, Several Names 158

The 2014 Data Breach: The Unique Malware of the Axiom Group 159

Malware Discovered during the 2015 Data Breach 162

2014 & 2015: Likely Connected, Possibly Coordinated 168

Chapter 7: OPM's OCIO and its Federal Watchdog 173

The IG's Memorandum of Concern 174

Four Instances Where the OCIO Failed to Cooperate Fully 177

Seymour failed to appropriately notify the IG of the April 2015 intrusion detection 177

Seymour failed to notify the OIG of the loss of background investigation data in a timely manner 180

Seymour failed to notify the OIG about the 2014 incident 182

Meetings with Federal Law Enforcement Agencies 183

KeyPoint Audit 184

Notification Concerning New IT Infrastructure 185

Five Incorrect and/or Misleading Statements 187

First Misstatement before the Senate Committee on Appropriations 187

Second Misstatement Before the Senate Committee on Appropriations 188

Third Misstatement Before Senate Committee on Appropriations and House Committee on Oversight and Government Reform 188

Fourth Misstatement Before the House Committee on Oversight and Government Reform 189

Fifth Misstatement Before the Senate 189

Current State of Relationship 189

Summary of OIG and OCIO relationship 193

Chapter 8: The IT Infrastructure Improvement Project: Key Weaknesses in OPM's Contracting Approach 194

The IG Issues a Flash Audit Alert and Interim Reports on the IT Infrastructure Project 196

The IG's Concerns Continued through the Fall of 2015 198

IG Reports Progress in Responding to Concerns, but Challenges Remain as of May 2016 198

The Story of OPM's IT Infrastructure Improvement Project and the Sole Source Contract 200

Timeline: OPM's IT Infrastructure Improvement Project 201

OPM Initiates Contact with Imperatis and Awards Sole Source Contract 205

Imperatis and OPM Buy Security Tools to Secure the Legacy IT Environment 206

Imperatis' Role in Responding to OPM Data Breach Incidents 207

Sole Source, Schedule, and Cost IG Concerns Related to OPM's IT Infrastructure Improvement Contract Validated 208

Summary of Investigation 214

Committee hearings on the data breaches 214
Committee request for information regarding identity theft services 215
Productions related to the OPM data breaches and CyTech 216
The Committee investigated the role of Cylance 219
The Committee investigated the role of SRA 220
The Committee Investigated OPM's IT Infrastructure Improvement Project and the Contract Awardee Imperatis 221
Document productions by Department of Homeland Security 221
Unnecessary delays, restrictions, redactions and a congressional subpoena 222
Unnecessary delays 222
Unnecessary redactions 222
Subpoena issued to OPM 224
Conclusion 225
Appendix: Cyber security Spending at OPM (Fiscal Years 2012-2015) 227

Timeline of Key Events

July 2012

- ✓ Attackers had access to OPM's network, according to US-CERT.[1] US-CERT found malware (Hikit) resided on an OPM server since 2012.[2]

November 2013

- ✓ First evidence of adversarial activity by the attacker associated with the breach that US-CERT informed OPM about in March 2014.[3]

December 2013

- ✓ First evidence of adversarial activity associated with the 2015 breaches (including harvesting of credentials from OPM contractors) by the attacker that was not identified until April 2015.[4]

March 20, 2014

- ✓ US-CERT notifies OPM of a data exfiltration from OPM's network.[5] OPM, working with US-CERT, determines and implements a strategy to monitor the attackers' movements to gather counterintelligence. This breach involved data that included manuals and IT system architecture information, but the full extent of exfiltrated data is unknown.

- ✓ The strategy remains in place until the "Big Bang" on May 27, 2014.

March 25, 2014

- ✓ Situation report takes place with CIO Donna Seymour and US-CERT.[6]

March 27, 2014

- ✓ As OPM monitors the hackers, it develops a "Plan for full shut down [of systems] if needed."[7]

[1] June 2014 OPM Incident Report at HOGR0818-001235 (OPM Production: Sept. 18, 2015) [hereinafter June 2014 OPM Incident Report]. Note: This Report was authored by DHS/US-CERT and provided to OPM.

[2] U.S. Dep't of Homeland Security/US-CERT, Digital Media Analysis Report-465355 (June 9, 2015) at HOGR0724-001154 (US-CERT Production: Dec. 22, 2015) [Hereinafter June 9, 2015 DMAR].

[3] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer of the U.S. Office of Personnel Mgmt.).

[4] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016).

[5] June 2014 OPM Incident Report at HOGR0818-001240.

[6] *Id.*

[7] *Id.*

April 11, 2014

- ✓ Tactical mitigation strategies and security remediation plan developed for briefing to Donna Seymour.[8]

April 21, 2014

- ✓ OPM contractor (SRA) discovers a "specific piece of malware," which is brought to US-CERT's attention.[9]

April 25, 2014

- ✓ "opmsecurity.org" is registered to Steve Rogers, a.k.a. "Captain America."[10] The hackers later used this domain for command and control (C2) and data exfiltration.[11]

May 7, 2014

- ✓ The attacker later associated with exfiltrating background investigation data establishes their foothold into OPM's network. This attacker poses as a background investigations contractor employee (KeyPoint), uses an OPM credential, remotely accesses OPM's network, and installs PlugX malware to create a backdoor.[12]

- ✓ OPM did not identify the attacker's May 7 foothold despite the fact that OPM was monitoring and removing another attacker (that US-CERT had notified OPM about in March 2014).

May 27, 2014

- ✓ OPM shuts down its compromised systems in the "Big Bang" event in an effort to remove the attacker. This decision was made after OPM observed the attacker "load a key logger onto . . . several database administrators' workstations" and they got

[8] *Id.* at HOGR0818-001241.

[9] *Id.* at HOGR0818-001242.

[10] ThreatConnect Research Team, *OPM Breach Analysis*, THREATCONNECT (June 5, 2015), available at: https://www.threatconnect.com/opm-breach-analysis/; H. Comm. on Oversight and Gov't Reform, Transcribed Interview of Brendan Saulsbury, Senior Cyber Security Engineer, SRA, Ex. 4 (Feb. 17, 2016) [Hereinafter Saulsbury Tr.].

[11] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); Saulsbury Tr. at 59.

[12] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Jeff P. Wagner, U.S. Office of Personnel Mmgt., Dir. of Information Technology Operations at 127-128 (Feb. 18, 2016) [hereinafter Wagner Tr.; Dep't of Homeland Sec./US-CERT and Office of Pers. Mgmt., OPM Cybersecurity Events Timeline (Aug. 26, 2015), at HOGR020316-000760-UR-A (OPM Production: May 13, 2016) [hereinafter OPM Cybersecurity Events Timeline]; Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016). KeyPoint CEO testified that "there was an individual who had an OPM account who was a KeyPoint employee and [] the credentials of that individual were compromised to gain access to OPM." *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, Chief Exec. Officer, KeyPoint). The OPM Director of IT Security Operations [Wagner] explained that "a KeyPoint user credential [was] utilized for [the] initial vector infection," but that "user did not have administrative credentials, so the adversary utilized tactics in order to gain domain administrator credentials" to move through the environment and conduct operations-related activities. Wagner Tr. at 86.

"too close to getting access to the PIPs system," which held the background investigation data.[13]

- ✓ Meanwhile, the attacker that established a foothold on May 7, 2014 continues their presence on the OPM network.

June 5, 2014

- ✓ Malware is successfully installed on a KeyPoint web server; accounts differ as to whether or not administrator privileges were used to install this malware. [14]

June 10, 2014

- ✓ OPM CIO Donna Seymour testifies before the Senate Homeland Security and Governmental Affairs' Subcommittee on OPM's *Strategic Information Technology Plan* and does not disclose at this hearing the "manuals" breach discovered in March 2014.[15]

June 12, 2014

- ✓ OPM executes a Cylance product evaluation agreement that allowed it to test the functionality of both Cylance products (V and Protect) for a limited period of time.[16]

June 20, 2014

- ✓ Attackers conduct a remote desktop protocol (RDP) session, indicating contact with "important and sensitive servers supporting . . . background investigation processes." The remote session was not discovered until spring 2015. [17]

June 22, 2014

- ✓ DHS issues a final incident report for the OPM "manuals" breach first discovered on March 20, 2014.[18]

[13] Saulsbury Tr. at 25-26.

[14] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015). Note: KeyPoint maintains that "No unaccounted security tokens were used during the time the malware was operational on KeyPoint's network." The US-CERT Report of the KeyPoint intrusion disagrees stating that "a domain administrator account was used to install the malware on the web server. US-CERT reported that this "administrator account" had "full access privileges."

[15] *A More Efficient and Effective Government: Examining Federal IT Initiatives and the IT Workforce: Hearing Before the S. Subcomm. on the Efficiency and Effectiveness of Fed. Programs & the Fed. Workforce of the S. Comm. on Homeland Sec. & Gov't Affairs*, 113th Cong. (June 10, 2014).

[16] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Stuart McClure, Chief Exec. Officer, President & Founder, Cylance, Inc., Ex. 2 (Feb. 4, 2016) [hereinafter McClure Tr.].

[17] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Chris Coulter, Managing Dir. of Incident Response and Forensics (Feb. 12, 2016), Ex. 18 [hereinafter Coulter Tr.]

[18] June 2014 OPM Incident Report at HOGR0818-001233-46.

June 23, 2014

- ✓ US-CERT/OPM identifies this as first known adversarial access to OPM's mainframe.[19]

July – August 2014

- ✓ Attackers successfully exfiltrate the background investigation data from OPM's systems.[20]

July 9, 2014

- ✓ OPM acknowledges the March 2014 "manuals" breach to the *New York Times*.[21] This information had not previously been disclosed publicly.

- ✓ OPM states that no PII was lost in the breach and does not disclose the exfiltration of the manuals.

July 29, 2014

- ✓ "opmlearning.org" is registered to Tony Stark, a.k.a. "Iron Man."[22] The attackers used this domain for command and control during their intrusion into OPM's environment.

August 16, 2014

- ✓ The malware installed on KeyPoint systems on June 5, 2014 ceased operational capabilities.[23]

October 2014

- ✓ FBI Cyber Division issues a Cyber Flash Alert regarding "a group of Chinese Government affiliated cyber actors who routinely steal high value information from US commercial and government networks through cyber espionage" and notes

[19] Dep't of Homeland Sec./US-CERT Briefing to Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.
[20] Id.
[21] Michael S. Schmidt, David E. Sanger & Nicole Perlroth, *Chinese Hackers Pursue Key Data on U.S. Workers*, N.Y. TIMES, July 9, 2014, available at: http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html?hp&action=click&pgtype=Homepage&version=LedeSum&module=first-column-region&region=top-news&WT.nav=top-news&_r=2.
[22] ThreatConnect, *OPM Breach Analysis*; Saulsbury Tr., Ex. 4.
[23] Letter from KeyPoint Government Solutions to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (July 2, 2015) (citing US-CERT Report (Aug. 30, 2014)). KeyPoint notes that "significantly, the malware was a "zero day" attack—it had an electronic signature that was not known by anti-virus/anti-malware software at that time."

activity associated with this group "should be considered an indication of a compromise requiring extensive mitigation…."[24]

✓ Meanwhile, the attackers move through the OPM environment to the U.S. Department of Interior (DOI) data center where OPM personnel records are stored.[25]

November 2014

✓ A group of private-industry security companies warns about threats to the human resources components of federal government and releases a report on Chinese Advanced Persistent Threat (APT) activity.[26]

December 2014

✓ 4.2 million personnel records are exfiltrated after attackers moved around OPM's system and through the DOI's database, which holds OPM personnel records.[27]

March 3, 2015

✓ "wdc-news-post[.]com" is registered by attackers. Attackers would use this domain for C2 and data exfiltration in the final stage of the intrusion.[28]

March 9, 2015

✓ The last beaconing activity to the unknown domain "opmsecurity.org" occurs. This domain was registered in April 2014 to Steve Rogers, a.k.a. "Captain America."[29]

March 26, 2015

✓ Fingerprint data appears to have been exfiltrated on or around this date.[30]

[24] Cyber Div., Fed. Bureau of Investigation, A-000042-MW, *FBI Cyber Flash Alert* (Oct. 15, 2014), http://www.slideshare.net/ragebeast/infragard-hikitflash.

[25] OPM Cybersecurity Events Timeline.

[26] Novetta, *Operation SMN: Axiom Threat Actor Group Report* 9 (2014), http://www.novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf (The report emphasizes "Hikit" malware, stating, "Among the industries we observed targeted or potentially infected by Hikit [included] Asian and Western government agencies responsible for [a variety of services such as] Personnel Management.").

[27] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

[28] DOMAIN > WDC-NEWS-POST.COM, THREATCROWD.ORG (last visited June 28, 2016), available at: https://www.threatcrowd.org/domain.php?domain=wdc-news-post.com .

[29] Saulsbury Tr. at 59.

[30] June 9, 2015 DMAR at HOGR0724-001158; *see also* Dep't of Homeland Sec./US-CERT Briefing to Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

April 15, 2015

- ✓ After being alerted by an OPM contractor (SRA) working on IT security, OPM notifies US-CERT about suspicious network traffic related to opmsecurity.org.[31] This domain was registered to Steve Rogers, a.k.a. "Captain America" in April 2014 and the last beaconing activity occurred in March 2015.

April 16, 2015

- ✓ OPM contacts Cylance for technical support on use of Cylance V, which was an endpoint detection tool that OPM had purchased in September 2014.[32] Cylance V is not intended to be an enterprise-wide prevention tool.[33]

April 17, 2015

- ✓ OPM begins to deploy enterprise-wide (on a demonstration basis and in "Alert" mode) a Cylance tool called CylanceProtect. At this time CylanceProtect was not in quarantine mode, but the tool would later identify and alert OPM to the widespread presence of malware on their system. OPM brings Cylance onsite for incident response.[34] OPM does not upgrade this tool to the highest preventative setting.[35]

April 18-19, 2015

- ✓ CylanceProtect is deployed to over 2,000 devices as of this date, makes "tons of findings," and as a Cylance engineer described the tool, it "lit up like a Christmas tree" indicating widespread malicious activities within the OPM system.[36]

April 21, 2015

- ✓ CyTech Services arrives onsite to conduct a product demonstration with their CyTech Forensics and Incident Response (CyFIR) tool, and remains onsite until May 1, 2015 to assist with incident response.[37]

April 22, 2015

- ✓ Then-CIO Donna Seymour testifies before the Committee about cybersecurity and publicly discussed the discovery of the "manuals" breach saying, "the adversaries in today's environment are typically used to more modern technologies, and so in this case, potentially, our antiquated technologies may have helped us a little bit. But I

[31] June 9, 2015 DMAR at HOGR0724-001158.
[32] Coulter Tr., Ex. 1, 2.
[33] McClure Tr. at 8.
[34] McClure Tr. at 21-22.
[35] *Id.* OPM upgraded from the *Cylance V* tool to the *Cylance PROTECT* tool. However, the tool remains in "Alert" mode only, not "Quarantine mode."
[36] McClure Tr., Ex. 8; Coulter Tr. at 20-21.
[37] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Benjamin Cotton, CyTech Services, Chief Executive Officer at 14-15 (Sept. 30, 2015) [hereinafter Cotton Tr.].

think also it comes down to culture and leadership, and one of the things that we were able to do at OPM was to recognize the problem."[38]

- ✓ OPM's Office of the Inspector General (OIG) learns of the breach for the first time after a staffer bumped into the OPM Director of Security Operations in the hallway.
- ✓ The staffer testified that OPM's Director of IT Security Operations said there was "no need" to notify the public of the breach.[39]

April 23, 2015

- ✓ OPM determines there had been a "major incident" involving the exfiltration of personnel records, which triggers a requirement to notify Congress.[40]
- ✓ OPM notifies Congress of a "major incident" on April 30, 2015.[41]

April 24, 2015

- ✓ OPM orders a global quarantine to address malware identified by CylanceProtect.[42]

April 26, 2015

- ✓ Cylance engineers identify adversarial activity related to an RDP session to a background investigation database indicating this session took place in June 2014.[43]

May 8, 2015

- ✓ US-CERT establishes with a high degree of certainty that personnel records data/PII had been stolen.[44]

May 20, 2015

- ✓ OPM determines there was a major incident regarding the exfiltration of background investigation data, which triggers a requirement to notify Congress.
- ✓ OPM notifies Congress on May 27, 2015.[45]

[38] *Enhancing Cybersecurity of Third-Party Contractors and Vendors: Hearing Before the H. Comm. on Oversight & Gov't. Reform,* 114th Cong. (Apr. 22, 2015) (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.) (testifying that OPM was hacked and that no PII was taken). The word "manuals" is not used at this time, though it is how we have since described the 2014 breach.

[39] H. Comm. on Oversight & Gov't Reform, Transcribed Interview of U.S. Office of Pers. Mgmt. Office of Inspector Gen. Special Agent at 17-18 (Oct. 6, 2015) [hereinafter Special Agent Tr.].

[40] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073, 3080 (2014).

[41] OPM Cybersecurity Events Timeline.

[42] Coulter Tr., Ex. 16.

[43] Coulter Tr., Ex. 18.

[44] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

✓ OPM indicates to the OIG that background investigation information may also be compromised.[46]

June 4, 2015

✓ OPM briefs the media and releases a press statement that revealed the personnel records of 4.2 million former and current federal employees have been compromised.[47]

June 8, 2015

✓ US-CERT establishes with a high degree of certainty that background investigation data/PII has been exfiltrated and stolen.[48]

June 16, 2015

✓ Then-OPM Director Katherine Archuleta acknowledges that background investigation data may be compromised.[49]

June 24, 2015

✓ Then-CIO Donna Seymour testifies before the Committee and minimizes the importance of data removed in 2014 "Manuals" breach, saying "those documents were some outdated security documents about our systems and some manuals about our systems."[50]

June 29, 2015

✓ The American Federation of Government Employees (AFGE) files a class action suit against OPM.[51]

[45] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

[46] Special Agent Tr. at 46.

[47] U.S. Office of Pers. Mgmt., Press Release, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.

[48] Briefing by US-CERT to H. Comm. on Oversight & Gov't Reform Staff (Feb. 19, 2016); OPM Cybersecurity Events Timeline.

[49] *OPM: Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform,* 114th Cong. (June 16, 2015) (statement of Katherine Archuleta, Dir., U.S. Office of Pers. Mgmt.).

[50] *Hearing on OPM Data Breach: Part II* (statement of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[51] *American Federation of Government Employees v. U.S. Office of Pers. Mgmt.*, No. 1:15-cv-1015 (D.D.C. filed June 29, 2015).

June 30, 2015

- ✓ After 74 days of deployment to over 10,250 devices, CylanceProtect detected and blocked almost 2,000 pieces of malware (including critical samples related to the breach)—nearly one piece of malware for every five devices.

July 9, 2015

- ✓ OPM issues a press release confirming background investigation data for 21.5 million individuals was compromised.[52]

July 10, 2015

- ✓ OPM Director Katherine Archuleta resigns.

July 21, 2015

- ✓ The Committee sends the first of a series of document requests to OPM.

August 20, 2015

- ✓ OPM returns the CyFIR tool to CyTech with key information deleted. The CyFIR tool, before it was deleted, contained images from OPM's incident response of more than 11,000 files and directories.

September 23, 2015

- ✓ OPM updates its original estimate that 1.1 million fingerprint records were compromised. The new estimate: 5.6 million.[53]

February 22, 2016

- ✓ Prior to testifying before the Committee, OPM CIO Donna Seymour resigns.

February 24, 2016

- ✓ Committee's planned hearing, "OPM Data Breach: Part III", is cancelled in the wake of OPM CIO Donna Seymour's resignation.[54]

[52] Press Release, U.S. Office of Pers. Mgmt., *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats* (July 9, 2015) available at: https://www.opm.gov/news/releases/2015/07/OPM-Announces-Steps-to-Protect-Federal-Workers-and-Others-From-Cyber-Threats/.

[53] Press Release, U.S. Office of Pers. Mgmt., *Statement by OPM Press Secretary Sam Schumach on Background Investigations Incident* (Sept. 23, 2015) available at: https://www.opm.gov/news/releases/2015/09/cyber-statement-923/.

[54] *OPM Data Breaches: Part III: Hearing Before H. Comm. on Oversight & Gov't Reform,* 114th Cong. (Feb. 24, 2016) (hearing cancelled).

Findings

Chapter 1: Findings Related OPM IT Security Record

OPM has long been plagued by a failure of management to prioritize information security in practice, and to retain leaders that are committed to information security over the long haul.

FINDING: OPM leadership failed to heed repeated recommendations from its Inspector General (IG). OPM has historically maintained a fragmented IT infrastructure, and still lacks a full, accurate inventory of all its major IT systems. As the IG noted in its FY2015 audit, "failure to maintain an accurate inventory undermines all attempts at securing OPM's information systems."

FINDING: Over the 2005-2015 timeframe, OPM failed to sufficiently respond to growing threats of sophisticated cyber attackers.

FINDING: OPM failed to prioritize resources for cyber security. In FY 2013, FY 2014 and FY 2015, OPM spent seven million each year on cybersecurity—spending that was consistently at the bottom relative to all other agencies that are required to report such expenditures to the Office of Management and Budget.

FINDING: Slow implementation of critical security requirements such as dual factor authentication is a true case of misplaced priorities.

FINDING: As early as 2005, OPM's IG issued a warning in a semiannual report that given the sensitive data OPM holds on former and current federal employees and family members, any attack or breakdown "could compromise efficiency and effectiveness and ultimately increase the cost to the American taxpayer."

FINDING: Key OPM systems, including the Personnel Investigations Processing System (PIPS), Enterprise Server Infrastructure (ESI), and the Local Area Network/Wide Area Network (LAN/WAN) were all operating on expired Authorities to Operate at the time of the data breach.

Chapter 2: Findings Related to the OPM Data Breach Discovered in 2014

In the spring of 2014 OPM suffered a data breach that resulted in the loss of documents relating to the most valuable databases on OPM's IT environment.

FINDING: Due to security gaps in OPM's network and a failure to adequately log network activity, the country will never know with complete certainty all of the documents that the attackers exfiltrated from OPM in connection with the breach discovered in March of 2014.

FINDING: The 2014 attackers used an uncommon toolkit designed for late-stage persistence and data exfiltration. The malware observed on OPM's systems in 2014 were two variants of Hikit malware, termed Hikit A and Hikit B.

FINDING: During an approximately two-month period, OPM watched the adversaries take sensitive data relating to high-valued targets on OPM's systems, including the server that holds background investigation materials, but was never able to determine how the adversary initially gained entry into their network.

FINDING: The documents taken by the 2014 attackers included information about OPM's systems that would have given an adversary an advantage in hacking the background investigation database and other sensitive systems in OPM's environment.

Chapter 3: OPM Attempts to Mitigate the Security Gaps Identified in 2014 While Iron Man and Captain America Go to Work (May 2014 – April 2015)

FINDING: In June 2014, US-CERT issued an incident report with 14 observations and recommendations to address the security gaps identified after the 2014 "manuals" breach. US-CERT deemed OPM's network very insecure, insecurely architected, and found OPM had a significant amount of legacy infrastructure.

FINDING: US-CERT also said there was a gap in information technology leadership across OPM as an agency and that it was not uncommon for existing security policies to be circumvented to execute business functions while exposing the entire agency to unnecessary risk.

FINDING: Had OPM leaders fully implemented basic, required security controls – including multi-factor authentication – when they first learned attackers were targeting background investigation data, they could have significantly delayed or mitigated the data breach of background information.

FINDING: In April 2015, an OPM contract employee identified a domain ("opmsecurity.org") that was purposely named to emulate a legitimate looking website and upon further investigation found the domain had a randomized email address and was registered to Steve Rogers, a.k.a. "Captain America." This was one of the first indicators of compromise identified by OPM in April 2015.

Chapter 4: Findings Related to the Role of Cylance Inc.

Information security tools of Cylance Inc. detected critical malicious code and other threats to OPM in April 2015 and thereafter played a critical role in responding to the data breaches in 2015.

FINDING: While Cylance tools were available to OPM as early as June 2014, OPM did not deploy its preventative technology until April 2015 after the agency was severely compromised and the nation's most sensitive information was lost. Swifter action by OPM to deploy CylanceProtect would have prevented or mitigated the damage that OPM's systems incurred.

FINDING: Following the May 27, 2014 "Big Bang" remediation, OPM decided not to purchase and deploy CylanceProtect due to, as Cylance CEO Stuart McClure put it, "political challenges on the desktop," meaning overcoming the tensions between IT security and program functionality.

FINDING: On April 15, 2015, OPM found an indicator of compromise and turned to Cylance for assistance. Cylance tools immediately found the most critical samples of malicious code present at OPM related to the breaches and that correspond to findings of DHS US-CERT.

FINDING: As of April 18-19, 2015, CylanceProtect was deployed (in Alert mode) to over 2,000 devices, made "tons of findings," and as a Cylance engineer described the tool it "lit up like a Christmas tree" – indicating widespread malicious activities in OPM's IT environment.

FINDING: OPM's former Director, Katherine Archuleta and former CIO Donna Seymour made questionable statements under oath about OPM's use of a quarantine to isolate malware and malicious process during the incident response.

FINDING: OPM eventually purchased CylanceProtect on June 30, 2015, but only as it was about to lose access to the product (as the demonstration period was ending). Despite Cylance's proven value during the 2015 incident response, OPM failed to timely make payments.

Chapter 5: Findings Related to the Role of CyTech Services

On June 10, 2015, the Wall Street Journal (WSJ) reported that CyTech Services, Inc. network forensics platform "CyFIR" actually discovered that data breach at OPM in mid-April during a sales demonstration.

FINDING: CyTech, a service disabled veteran-owned small business contractor, did participate in several meetings with OPM in early 2015 to discuss the capabilities of their CyTech Forensics and Incident response (CyFIR) tool and provided a demonstration of their CyFIR tool on April 21, 2015 at OPM headquarters.

FINDING: During the April 21 demonstration CyTech did identify malware on the live OPM IT environment related to the incident. CyTech was not aware at the time that OPM had identified on April 15 an unknown Secure Sockets Layer (SSL) certificate beaconing to a malicious domain (opmsecurity.org) not associated with OPM.

FINDING: Beginning on April 22, 2015, CyTech offered and began providing significant incident response and forensic support to OPM related to the 2015 incident.

FINDING: CyTech did not leak information about their involvement with the OPM incident to the press.

FINDING: The testimony given by the (now former) OPM CIO, Donna Seymour, before the Committee on June 24, 2015 regarding the CyTech matter is inconsistent with the facts on the record.

FINDING: Documents and testimony show CyTech provided a service to OPM and OPM did not pay. The Anti-deficiency Act (ADA) prohibits a federal agency from accepting voluntary services.

Chapter 6: Findings Related to the Connections between the 2014 and 2015 Intrusions at OPM

The data breaches OPM suffered in 2014 and 2015 share commonalities relevant not only to attribution, but more importantly OPM's reaction or lack thereof in the wake of the 2014 intrusion.

FINDING: The data breach discovered in March 2014 was likely conducted by the Axiom Group. This conclusion is based on the presence of Hikit malware and other Tactics Techniques and Procedures (TTPs) associated with this group, which have been publicly reported.

FINDING: The data breaches discovered in April 2015 were likely perpetrated by the group Deep Panda (a.k.a. Shell_Crew, a.k.a. Deputy Dog) as part of a broader campaign that targeted federal workers. This conclusion is based on commonalities in the 2015 adversary's attack infrastructure and TTPs common to other hacks publicly attributed to Deep Panda. These groups include Wellpoint/Anthem, VAE Inc., and United Airlines. However, the cyber intrusion and data theft announced by Anthem in 2015 is a separate attack by a separate threat actor group unrelated to the hack against OPM discovered in 2015.

FINDING: As publicly reported, both the Axiom and Deep Panda groups are highly likely to be state-sponsored threat-actor group supported by the same foreign government.

FINDING: It is highly likely that the 2014 and 2014/2015 cyber intrusions into OPM's networks were likely connected and possibly coordinated campaigns.

Chapter 7: Findings Related to the Relationship between the OPM OCIO and its IG

Federal watchdogs play a critical role in the federal government, partnering with agencies to improve and safeguard programs and operations, including during and after data breaches.

FINDING: The relationship between the OPM Office of the Inspector General (OIG) and Office of the Chief Information Officer (OCIO) became strained during the tenure of former Director Katherine Archuleta and former CIO Donna Seymour. The relationship became so strained that on July 22, 2015, then-Inspector General Patrick McFarland issued a memorandum to OPM's Acting Director Beth Cobert to share "serious concerns" regarding the OCIO.

FINDING: Former OPM Director Katherine Archuleta and former OPM CIO Donna Seymour engaged in activities that hindered the work of the OIG, including when:
(1) OPM's OCIO failed to timely notify the OIG of the 2014 and 2015 data breaches or the data that was compromised;
(2) Director Archuleta stated that the OIG could not attend certain meetings relating to the data breaches because the OIG's presence would "interfere" with the FBI and US-CERT's work;
(3) The OCIO failed to notify and involved OIG in a major IT investment to develop a new IT infrastructure; and
(4) The OIG delayed an audit of KeyPoint Government Solutions at the request of the OCIO after an October 16, 2014 meeting, only to learn later OPM knew in early September 2014 that KeyPoint had been breached and did not disclose this information to the OIG.

FINDING: Former OPM Director Katherine Archuleta and former OPM CIO Donna Seymour made five incorrect and/or misleading statements to Congress. These statements were:
(1) Director Archuleta testified June 23, 2015 before the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, that OPM completed a Major IT Business Case (formerly known as the OMB "Exhibit 300") for the infrastructure improvement project; contrary to the finding of the OPM OIG;

(2) At the same June 23, 2015 hearing, Director Archuleta testified that "my CIO has told me that we have, indeed, an inventory of systems and data," contrary to the findings of the OIG in both a flash audit alert and the FY 2014 FISMA audit;
(3) Director Archuleta and CIO Donna Seymour testified before the Senate Appropriations Committee and the House Committee on Oversight and Government Reform that the sole-source contract with OPM's contractor (Imperatis) for the IT Infrastructure Improvement project covered only the first two phases of this multiphase IT Infrastructure Improvement project, and contracts for the later phases (migration and cleanup) of the project had not been awarded. However, the OIG found that the sole-source contract provided for work under all four phases of the project;
(4) OPM CIO Seymour testified before the House Committee on Oversight and Government Reform on June 16, 2015 that the 11 OPM systems operating without authorization were no longer a concern because she had granted an interim authorization to these systems. However, the IG found that OMB does not allow interim or extended authorizations; and
(5) At a June 25, 2015 hearing held by the Senate Committee on Homeland Security and Governmental Affairs, Director Archuleta stated that OPM had received a special exemption from OMB related to system authorization because of the ongoing IT Infrastructure Improvement project; however, this claim could not be substantiated.

FINDING: The relationship between the OPM OIG and OPM leadership has improved under Acting Director Beth F. Cobert.

Chapter 8: Findings Related to the IT Infrastructure Improvement Project

In response to the data breach at OPM in 2014, and after identifying serious vulnerabilities in the OPM network, the agency, at the recommendation of DHS, initiated the IT Infrastructure Improvement project.

FINDING: OPM's IT Infrastructure Improvement project is a case study illustrating why agencies need to ensure robust communications with the OIG, particularly in responding to cybersecurity incidents. Former OPM CIO Seymour said she was not aware of a requirement "to notify the IG of every project that we take on."

FINDING: OPM's use of a sole-source contract in an emergency situation illustrates why there should be pre-established contract vehicles for cyber incident response and related services.

FINDING: There is a pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end of life IT systems and applications.

Recommendations

In 2015 OPM announced the largest data breach of personally identifiable information (PII) of 22.1 million Americans. This failure of culture and leadership cannot happen again. The federal government must recognize and mitigate the ever-increasing cyber threat and protect the information that Americans entrust to the government. While there was much that went wrong for years in the federal government's approach to information security, this episode presents an opportunity for Congress and other agencies to inject new leadership and a culture of security in federal IT. The recommendations listed below are aimed at taking lessons learned from the OPM experience and charting a path of ever vigilant IT security in order to secure the PII of Americans held by the federal government.

Recommendation 1 – Ensure Agency CIOs are Empowered, Accountable, and Competent

Each federal agency must ensure agency CIOs are empowered, accountable, competent and retained for more than the current average two year tenure. The CIO at federal agencies and independent executive agencies is a critical leader who should be accountable to the head of the agency. Under federal laws, such as the Federal Information Security Management Act (FISMA) and the Federal Information Technology Acquisition Reform Act (FITARA), CIOs are responsible for IT security and management functions within the agency. In the last two years, Congress revised FISMA and FITARA to reflect the new prioritization agency heads should place on IT management and security. CIOs typically serve an average of two years, but greater priority should be placed on retaining these leaders for at least five years.[55] This Committee, and in particular the IT subcommittee, has made IT management and security an oversight priority to ensure vigorous implementation of FISMA and FITARA. Such oversight has included a FITARA scorecard to assess agencies' implementation of this law. This oversight will continue and agencies will be expected to ensure there is an empowered, accountable, and competent CIO serving in this critical role.

Recommendation 2 – Reprioritize Federal Information Security Efforts Toward a Zero Trust Model

OMB should provide guidance to agencies to promote a zero trust IT security model. The OPM data breaches discovered in 2014 and 2015 illustrate the challenge of securing large, and therefore high-value, data repositories when defenses are geared toward perimeter defenses. In both cases the attackers compromised user credentials to gain initial network access, utilized tactics to elevate their privileges, and once inside the perimeter, were able to move throughout OPM's network, and ultimately accessed the "crown jewel" data held by OPM. The agency was unable to visualize and log network traffic which led to gaps in knowledge regarding how much data was actually exfiltrated by attackers.

To combat the advanced persistent threats seeking to compromise or exploit federal government IT networks, agencies should move toward a "zero trust" model of information security and IT

[55] Gov't Accountability Office, GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (Oct. 2011) (stating the average CIO's tenure is two years).

architecture. The zero trust model centers on the concept that users inside a network are no more trustworthy than users outside a network.[56] The zero trust model requires strictly enforced user controls to ensure limited access for all users and assumes that all traffic traveling over an organization's network is threat traffic until authorized by the IT team. In order to effectively implement a zero trust model, organizations must implement measures to visualize and log all network traffic, and implement and enforce strong access controls for federal employees and contractors who access government networks and applications.

Recommendation 3 – Reduce Use of SSNs by Federal Agencies

Federal agencies should reduce the use of Social Security Numbers (SSN) in order to mitigate the risk of identity theft. SSNs are key pieces of PII that can potentially be used to perpetrate identity theft. The potential for misuse of SSNs has raised questions about how the federal government obtains, uses, and protects the SSNs it obtains. In May 2007, OMB required all federal agencies to review their use of SSNs in agency systems and programs in order to identify opportunities to reduce such use.[57] Agencies were required to establish a plan, within 120 days of the memo, to eliminate the unnecessary collection and use of SSNs within 18 months. They were also required to participate in government-wide efforts to explore alternatives to the use of SSNs as a personal identifier for federal employees and in the administration of federal programs. In response to a 2016 request by Chairman Chaffetz, the U.S. General Accountability Office (GAO) is currently reviewing actions agencies have taken to reduce the use of SSNs government-wide, actions OMB has taken to ensure agencies have adhered to its directive, and what progress has been made in reducing the use of SSNs across the federal government. Congress should carefully monitor the progress of these important actions, and work with agencies to ensure steps are taken to efficiently and effectively reduce agency use of SSNs.

Recommendation 4 – Require Timely Justifications for Lapsed Authorities to Operate

Agencies that fail to re-authorize the authorities to operate (ATO) for their critical federal systems should be required to provide Congress, within 15 days of the system's authorization expiring, a justification as to why the system authorization was allowed to lapse. Designated critical information systems lacking adequate justification for a lapsed ATO should be removed immediately from the production environment.

ATOs provide a comprehensive assessment of the IT system's security controls and are a vital part of ensuring federal systems operate securely. FISMA requires agencies to assess the effectiveness of their information security controls, the frequency of which is based on risk but no less than annually. OMB Circular A-130, Appendix III required agencies to assess and authorize (formerly referred to as certify and accredit) their systems before placing them into operational environment and whenever there is a major change to the system, *but no less than*

[56] This model was proposed by Forrester Research Inc., an American-owned independent research and advisory firm. in response to a 2013 National Institute of Science and Technology (NIST) request for information entitled, "Developing a Framework to Improve Critical Infrastructure Cybersecurity" NIST RFI# 130208119-3119-01. *See* 78 Fed. Reg. 13024 (Feb. 26, 2013) available at: http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf.

[57] Memorandum from Office of Mgmt. & Budget, Exec. Office of the President, to the Heads of Exec. Dep'ts & Agencies, M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf.

every three years thereafter.[58] At OPM, critical systems were operating in FY 2014 without a valid ATO.[59] Of the 21 OPM systems due for reauthorization in FY 2014, 11 were not completed on time and were operating without a valid authorization,[60] and several were among the most critical, containing the agency's most sensitive information.[61] This led the IG to warn OPM that "[t]he drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own."[62] A failure to maintain current ATOs negatively impacts the security of federal information systems. As the OPM IG pointed out, "there are currently no consequences for OPM systems that do not have a valid Authorization to operate."[63]

Consequently, agencies should account for lapses to Congress and be prepared to take critical systems out of production. Further, at OPM, the IG recommended the adoption of administrative sanctions for the failure to meet security authorization requirements.[64] Congress and the Administration should consider options (including legislation or policy guidance) to ensure there are appropriate consequences for lapsed ATOs.

Recommendation 5 – Ensure Accountability and Empower DOD IT Officials Implementing Necessary Security Improvements for NBIB

Clear rules for accountability and dedicated funding should be established by the end of FY 2017 to ensure the U.S. Department of Defense (DOD) is successful in securing the background investigation materials that will now be held at the new National Background Investigations Bureau (NBIB). In an effort to reform the background investigation process and secure related data, this function will now reside at the new NBIB and the DOD CIO will be responsible for IT.[65] The DOD CIO has testified that he will ultimately answer to the Secretary of Defense in matters relating to NBIB and that DOD will provide short-term funding for IT at NBIB.[66]

[58] Office of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, Management of Federal Information Resources (Nov. 28, 2000) available at: https://www.whitehouse.gov/omb/circulars_a130_a130trans4/. OMB Circular A-130 was recently updated and includes new guidance for agencies on Authorization to Operate and Continuous Monitoring. Office of Mgmt & Budget Exec. Office of the President, OMB Circular A-130 Management of Federal Information Resources (July 27, 2016) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf. The Committee expects to continue oversight in the areas covered by the revised A-130.

[59] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014* (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

[60] *Id.* at 9.

[61] E-mail from Inspector Gen. Staff, U.S. Office of Pers. Mgmt., to H. Comm. on Oversight & Gov't Reform Staff (Dec. 4, 2015) (on file with the Committee).

[62] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., Report No. 4A-CI -00-14-016, *Federal Information Security Management Act Audit FY 2014*, at 9 (Nov. 12, 2014) available at: https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[63] *Id.* at 10.

[64] *Id.* at 11.

[65] White House, Press Release, *The Way Forward for Federal Background Investigations* (Jan. 22, 2016), https://www.whitehouse.gov/blog/2016/01/22/way-forward-federal-background-investigations.

[66] *Security Clearance Reform: The Performance Accountability Council's Path Forward: Hearing Before the House Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 25, 2016) (testimony of Terry Halvorsen, Chief Info. Officer, U.S. Dep't of Defense).

However, it is not yet clear whether future IT funding for NBIB will come from DOD, OPM, or another source.[67] It is also unclear how disagreements between DOD and OPM regarding IT security spending would be resolved.[68] To ensure that IT security is appropriately prioritized at NBIB, OPM and DOD should establish clear sources of funding and decision-making processes for IT security, and the OIG at both OPM and DOD should work to oversee such implementation and management.

Recommendation 6 – Eliminate Information Security Roadblocks Faced by Agencies

To the extent there are non-security related bureaucratic hurdles to quickly implementing IT security policies and deploying cyber tools, agencies should make every effort to streamline processes and prioritize security. The federal government's most important responsibility is to protect this nation and our citizens – including when it comes to protecting this nation against cyberattacks. The process of deploying security tools can be cumbersome and requires navigating a bureaucratic process that may involve notifying unions and overcoming program manager opposition.[69] Congress should enact legislation sponsored by Rep. Gary Palmer in the House (H.R. 4361) and Senator Joni Ernst (S. 2975) to clarify agencies' authority under FISMA by stating the heads of federal agencies are able to take timely action to secure their IT networks, and without being required to first provide unions with the opportunity to bargain.

Recommendation 7 – Strengthen Security of Federal Websites and Breach Notifications

Congress should enact H.R. 451, the Safe and Secure Federal Websites Act of 2015, legislation sponsored by Rep. Chuck Fleischmann that increases the certification requirements for public federal websites that process or contain PII. The bill requires an agency's CIO to certify the website for security and functionality prior to making it publicly accessible. The bill also increases the requirements for agencies when responding to an information security breach that involves PII. The events that unfolded at OPM in 2014 and 2015 demonstrated an unwillingness by some officials to notify the public of a PII compromise in a timely manner. The bill directs OMB to develop and oversee implementation of the certification requirements, which include reporting the breach to a federal cyber security center and notifying individuals affected by a PII compromise.

Recommendation 8 – Financial Education and Counseling Services Through Employee Assistance Programs

Congress should encourage federal agencies to provide federal employees with financial education and counseling services that are designed to help employees recognize, prevent and mitigate identity theft through existing Employee Assistance Programs (EAP). An EAP is a voluntary, work-based program that offers free and confidential assessments, short-term

[67] *Id.*

[68] *Id.*

[69] In the case of OPM's efforts to deploy a tool called Forescout (which is a tool to manage network access control for devices), there were deployment delays due in part to the need to notify unions. Imperatis Weekly Report (Aug. 3, 2015-Aug. 7, 2015), Attach. 6 at 000942 (Imperatis Production: Sept. 1, 2015) (stating "project sponsor is in notification stage with the Union" and mitigation was to "prepare updated project timeline, plan & memo to pilot ForeScout to non-union agency users.").

counseling, referrals, and follow-up services to employees who have personal and/or work-related problems.[70]

Recommendation 9 – Establish Government-wide Contracting Vehicle for Cyber Incident Response Services

OMB and the General Services Administration (GSA) should lead efforts to establish a government-wide contracting vehicle for Cyber Incident Response Services or Congress should establish a statutory requirement for such a vehicle. After the data breach discovered in March 2014, OPM awarded a sole source contract for a multi-phased IT Infrastructure Improvement project. Under this contract, OPM procured cybersecurity tools to secure their legacy IT environment. Instead of duplicative sole source contracts across various agencies, the federal government should have pre-established contracting vehicles that have the benefit of competition and are available to provide incident response services, including tools to secure IT environments post-breach.

Agencies should not be in the process of establishing contracts for these services during the incident response period. In October 2015, OMB published a Cyber Security Strategy and Implementation Plan (CSIP) for the federal civilian government agencies.[71] The CSIP included a number of deliverables, including one related to establishing contracting vehicles providing incident response services. A government-wide contracting vehicle for incident response services should be established as soon as possible and *before* another agency faces the same situation as OPM. This will ensure such contracting vehicles have the benefit of competition and provide a robust suite of services to assist agencies in an incident response scenario.

Recommendation 10 – Improve and Update Cybersecurity Requirements for Federal Acquisition

OMB should refocus efforts on improving and updating the current patchwork and outdated cybersecurity requirements in existing federal security and acquisition rules. There have been a number of initiatives launched over the last few years to update and improve cybersecurity requirements in federal acquisition. To date, few of these efforts have been finalized. Thus, the Committee recommends that the Administration prioritize and complete efforts to develop and implement clear cybersecurity requirements for federal acquisition as soon as possible. The importance of the partnership between agencies and federal contractors in securing sensitive data held by agencies and contractor-operated systems cannot be overstated. Existing cybersecurity rules and requirements in federal acquisition are ad hoc, overlapping, potentially conflict and are in need of updating.

In February 2013, the President issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Reliance*, that directed agencies to complete a broad range of tasks to enhance national

[70] *What is an Employee Assistance Program*, U.S. OFFICE OF PERS. MGMT, available at: https://www.opm.gov/faqs/QA.aspx?fid=4313c618-a96e-4c8e-b078-1f76912a10d9&pid=2c2b1e5b-6ff1-4940-b478-34039a1e1174.

[71] Memorandum from Shaun Donovan, Dir., and Tony Scott, Fed. Chief Info. Officer, Office of Mgmt. & Budget, Exec. Office of the President, to Agency Heads, M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Oct. 30, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

cybersecurity and resilience.[72] One group of deliverables included a mandate to incorporate cybersecurity requirements into the federal acquisition process. In January 2014, GSA and DOD delivered a report, *Improving Cybersecurity and Reliance through Acquisition* that made recommendations to achieve this objective.[73] These report recommendations have not been implemented to date. The existing framework for cybersecurity requirements in federal acquisition should be reviewed and updated immediately. The January 2014 report recommendations provide useful guidance to inform such an update.

Recommendation 11 – Modernize Existing Legacy Federal Information Technology Assets

Federal agencies should utilize existing tools and Congress should consider new tools to incentivize the transition from legacy to modernized IT solutions. Federal agencies spend over $89 billion annually on IT, with the majority of this spending focused on maintaining and operating legacy IT systems.[74] Over 75 percent of this spending is focused on legacy IT costs.[75]

GAO reported legacy IT investments are becoming increasingly obsolete with outdated software languages and hardware parts that are not supported.[76] Such reliance on legacy IT can result in security vulnerabilities where old software or operating systems are no longer supported by vendors and aging IT infrastructure becomes difficult and expensive to secure. OPM testified before the Committee there "are some of our legacy systems that may not be capable of accepting those types of encryption…"[77]

The solution to this legacy IT challenge must be multifaceted and should include the use of existing and new tools to incentivize modernization. FITARA provides important tools for IT management and acquisition, including facilitating the transition from legacy IT to modernized solutions.[78] In terms of new tools, incentives for agencies to achieve savings through modernization and innovative financing options to promote modernization should be considered.

Recommendation 12 – Agencies Should Consider Using Critical Pay for IT Security Specialists:

Agencies may request and be granted "critical position pay" authority. Agencies may request critical position pay authority only after determining the position in question cannot be filled

[72] Exec. Order No. 13636, 78 Fed. Reg. 11739 (Feb. 19, 2013); White House, Press Release, Presidential Policy Directive 21, *Critical Infrastructure Security and Reliance* (Feb. 12, 2013).

[73] Gen. Serv's Admin. & Dep't of Defense, *Improving Cybersecurity and Resilience Through Acquisition* (Nov. 2013), available at: http://www.gsa.gov/portal/mediaId/185367/fileName/improving_cybersecurity_and_resilience_through_acquisition.action.

[74] The annual total of $89 billion for IT understates the federal government's total IT investment because it does not include: (1) DOD classified IT systems; (2) IT investments by 58 independent executive branch agencies (including the CIA); and (3) IT investments by the legislative or judicial branches. Data available through the IT Dashboard, https://itdashboard.gov/ and OMB Office of E-Gov and Information Technology, https://www.whitehouse.gov/omb/e-gov/docs.

[75] Gov't Accountability Office, GAO-16-468, *Information Technology Federal Agencies Need to Address Aging Legacy Systems*, (May 2016).

[76] Id.

[77] *OPM Data Breach: Hearing Before the H. Comm. on Oversight & Gov't Reform* (June 16, 2015) (testimony of Donna Seymour, Chief Info. Officer, U.S. Office of Pers. Mgmt.).

[78] National Defense Authorization Act FY 2015, Pub. L. No. 113-291, Title VIII, Subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014).

with an "exceptionally well-qualified individual" through the use of other available human resource flexibilities and pay authorities. OPM, in consultation with OMB, reviews agency requests. When approving a request, OPM must determine whether the position requires an "extremely high level of expertise" in a "scientific, technical, professional, or administrative field" and is mission critical. Authority is used to *recruit* and/or *retain* exceptional talent, and is capped at 800 positions at any one time. Generally, critical pay may be established up to Cabinet Secretary pay levels ($205,700) and can be increased with approval by the President (but pay and bonus generally cannot exceed the vice president's salary).

The Committee intends to collect more information on the use of critical pay authority in order to conduct appropriate oversight and make adjustments to the authority, and to ensure it provides agencies the necessary flexibility for recruitment and retention of IT security talent. OPM should also consider establishing a pay band for Information Technology Security Specialists.

Recommendation 13 – Improve Federal Recruitment, Training and Retention of Cyber Security Specialists

Recruiting, training, and retaining cyber security specialists should be a critical national security priority. Following the cyberattacks at OPM, the federal CIO and the OMB Director issued a Memorandum concerning a cybersecurity strategy and implementation plan (CSIP) for the federal civilian government.[79] The CSIP included several federal cyber workforce related taskings, including directing:

1. OPM and OMB to compile special hiring authorities by agency that can be used to hire cyber and IT professionals across government.

2. Agencies to participate in OPM's *Cyber Workforce Project* – an effort to code cybersecurity jobs by specialty for the purpose of gaining knowledge about the gaps and challenges in cyber recruitment and retention.

3. DHS to pilot an Automated Cybersecurity Position Description Hiring Tool to assist in implementation of the National Initiative for Cybersecurity Education (NICE) framework, and posting analysis of the cyber workforce on the CIO Council's knowledge portal as a best practice for other agencies to follow.

4. OPM, DHS, and OMB to map the entire cyber workforce across all agencies using the NICE National Cybersecurity Workforce Framework.

5. OPM, DHS, and OMB to develop recommendations for federal workforce training and professional development.

The Administration and Congress must work together to complete these tasks and swiftly take the steps needed to recruit, train, and retain a world class cyber workforce. The Committee notes

[79] Memorandum from Shaun Donovan, Dir., and Tony Scott, Fed. Chief Info. Officer, Office of Mgmt. & Budget, Exec. Office of the President, to Agency Heads, M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government* (Oct. 30, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

OMB and OPM jointly transmitted a memorandum to agency heads on a Federal Cybersecurity Workforce Strategy on July 12, 2016 and appreciates this opportunity to continue the dialogue in this area. Finally, Congress and the Administration should consider non-traditional mechanisms to recruit and retain cyber talent. Such mechanisms should complement private sector experience rather than compete with the private sector, recognize the need to quickly hire top talent, and provide an opportunity for public service to those in the private sector.

Table of Names

Office of Personnel Management

Name	Title
Katherine L. Archuleta	Director (May 2013 - July 2015)
Morrell John Berry	Director (April 2009 - April 2013)
Beth F. Cobert	Acting Director (July 2015 - present)
Jason K. Levine	Director of Office of Congressional, Legislative, and Intergovernmental Affairs (August 2015 - present)
Patrick E. McFarland	Inspector General (August 1990-February 2016)
Lisa Schlosser	Acting Chief Information Officer (March - August 2016)
Donna K. Seymour	Chief Information Officer (December 2013-February 2016)
Special Agent in Charge	Office of Inspector General
Linda M. Springer	Director (June 2005-2008)
Clifton ("Clif") N. Triplett	Senior Cyber and Information Technology Advisor
Norbert ("Bert") E. Vint	Acting Inspector General (February 2016 - present) Deputy Inspector General (2006-February 2016)
Jeff P. Wagner	Director of Information Technology Security Operations

Assurance Data, Inc.

Name	Title
Matthew Morrison	President and Chief Executive Officer

Cylance Inc.

Name	Title
Chris Coulter	Managing Director of Incident Response and Forensics
Stuart McClure	Chief Executive Officer, President and Founder
Grant Moerschel	Director of Sales Engineering
Nicholas Warner	Vice President of Worldwide Sales

CyTech Services

Name	Title
Juan Bonilla	Sr. Security Consultant Solutions Engineering (with OPM April 23-May 1, 2015)
Ben Cotton	Chief Executive Officer

SRA

Name	Title
Brendan Saulsbury	Senior Cyber Security Engineer (March 2012 - May 2016)
Jonathan Tonda	OPM Branch Chief, Security Engineering (September 2015-present); Network Security Team Lead, SRA (May 2012-September. 2015)

Imperatis

Name	Title
Patrick Mulvaney	Technical Lead for OPM contract

Misc.

Name	Title
Joel Brenner	Former National Security Agency Senior Counsel
James B. Comey, Jr.	Director of the Federal Bureau of Investigations
Michael V. Hayden	Former Director of the Central Intelligence Agency
James Andrew Lewis	Senior Vice President and Director, Strategic Technologies Program, Center for Strategic and International Studies
Jeff Neal	Former Chief Human Capital Officer at the U.S. Department of Homeland Security
John Schindler	Former National Security Agency officer
Richard A. Spires	Former Chief Information Officer at the U.S. Department of Homeland Security and the Internal Revenue Service

Chapter 1: OPM's IT Security Record Preceding Breaches

The attackers who successfully penetrated the U.S. Office of Personnel Management (OPM) network were sophisticated, but neither their methods nor their ambition was unprecedented. The federal government had been subject to attacks for years by the same or similar groups using similar variants of malware. In fact, OPM had reportedly been hacked in 2012. A vast amount of publicly available information on similar hacks within the past decade was available that should have put OPM on notice. Furthermore, OPM had every incentive to prioritize information security given the volume of sensitive information and PII it holds.

Despite red flags that began as early as 2005, OPM's appropriated IT security funding consistently lagged behind other agencies, its most sensitive data was inadequately protected, and OPM leadership failed to heed recommendations from OPM's IG.

The Rise of Advanced Persistent Threat Hacking

The longstanding OPM cyber security failures that culminated in the theft of personnel records, background investigation data, and fingerprint data began a decade earlier when the federal government was put on notice regarding the nature of the threat. In July 2005, the U.S. Computer Emergency Response Team (US-CERT) issued an alert regarding sophisticated, multi-year efforts in which hackers send targeted, socially-engineered emails (commonly called "spear phishing" emails) for the purpose of having a user download a file that would eventually lead to the exfiltration of sensitive information.[80]

Though the term would not emerge for several years, the alert described what would come to be known as an "advanced persistent threat" (APT) attack. Such attacks are focused on a particular set of high-value assets or physical systems with the explicit purpose of maintaining access and of stealing data over time. Because the attackers are sophisticated, they can learn how to jump from system to system within a given network, often attempting to compromise administrator accounts in order to gain wider and higher levels of access and creating new footholds to maintain their access. When a particular security precaution or obstacle prevents further compromise, the attackers change tactics and maintain a presence on the network until they reach their ultimate objective.

The 2005 US-CERT alert noted that APT attacks had already taken place, and that they often used malware specifically designed to elude anti-virus software and firewalls.[81] The alert specifically noted the use of "McAfee" and "Symantec" names in connection with APT hacks, foreshadowing the "McAfee" name that would later be relevant in the OPM breach.[82]

Since 2005, the federal government has been repeatedly victimized by sophisticated, sustained APT attackers. In 2005, an APT intrusion gathered data from NASA's Vehicle

[80] US-CERT, *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks* (July 2005).
[81] *Id.*
[82] *Id.*; *see also* Saulsbury Tr. at 60.

Assembly Building.[83] Media outlets reported that Chinese involvement in the hack was likely.[84] In 2007, James A. Lewis of the Center for Strategic and International Studies testified before Congress that intrusions occurred at the Defense Department, State Department and the Commerce Department.[85] In late 2014, a media report catalogued a number of recent attacks against federal entities, including the White House, the State Department, the United States Postal Service, OPM, and the Nuclear Regulatory Commission.[86]

Federal Contractors Holding Sensitive Federal Employee Information Targeted and Attacked

In addition to the targeting of federal agencies, the government contractors that provide services to these agencies and hold sensitive federal employee information increasingly have been targeted by APTs, including several OPM contractors that provide background investigation and healthcare services. The first public reports of data breaches involving OPM contractors surfaced in the summer of 2014.

In August 2014, the largest background investigation contractor, U.S. Investigations Services, LLC (USIS),[87] publicly acknowledged a data breach impacting employees of the Department of Homeland Security.[88] Documents and testimony provided to the Committee indicate that USIS "self-detected" this cyber-attack in June 2014, immediately notified OPM, and by early July 2014 had mitigated the attackers' activity on their systems.[89]

In a June 22, 2015 document provided to the Committee, USIS said based on the results of an investigation, conducted by a company called Stroz Friedberg, it was determined that USIS had been the target of an attack "carried out by a state sponsored actor," commonly referred to as an APT attack.[90] USIS told the Committee that PII for over 31,000 individuals associated with

[83] Keith Epstein & Ben Elgin, *Network Security Breaches Plague NASA*, BUS. WEEK, Nov. 20, 2008.
[84] *Id.*
[85] *Holistic Approaches to Cybersecurity to Enable Network Centric Operations: Hearing before the Subcomm. On Terrorism, Unconventional Threats and Capabilities of the H. Comm. On Armed Serv.'s.*, 111th Cong. (Apr. 1, 2008) (statement of James Andrew Lewis).
[86] Jack Moore, *The Year of the Breach: 10 Federal Agency Data Breaches in 2014*, NEXTGOV (Dec. 30, 2014), http://www.nextgov.com/cybersecurity/2014/12/year-breach-10-federal-agency-data-breaches-2014/102066/.
[87] In 1996, USIS was established as a result of the privatization of OPM's Investigations Services and over the years was awarded a series of contracts to perform security clearance background investigations for more than 95 federal agencies. There were a variety of transition issues when the privatization first occurred, including questions about USIS employees' access to government databases. *See* General Accounting Office, GAO/GGD-96-97R, *Privatization of OPM's Investigations Service* (Aug. 22, 1996). In September 2014, OPM decided to end these contracts with USIS. In early 2015, USIS' parent company filed for bankruptcy. *See* Jill Aitoro, *It is Official: USIS is No More with Planned Altegrity Bankruptcy*, WASH. BUS. J., Feb. 4, 2015, http://www.bizjournals.com/washington/blog/fedbiz_daily/2015/02/it-s-official-usis-isno-more-with-planned.html.
[88] Ellen Nakashima, *DHS Contractor Suffers Major Computer Breach, Officials Say*, WASH. POST, Aug. 6, 2014, available at: https://www.washingtonpost.com/world/national-security/dhs-contractor-suffers-major-computer-breach-officials-say/2014/08/06/8ed131b4-1d89-11e4-ae54-0cfe1f974f8a_story.html.
[89] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Services. LLC).
[90] Letter from Counsel for U.S. Investigations Serv's, LLC (USIS) to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform (June 22, 2015); *Id*, Ex. 12, (Stroz Friedberg Summary of Investigation (Dec. 2014).

USIS background investigation work for Customs and Border Protection, the National Geospatial-Intelligence Agency, Immigration and Customs Enforcement, and the U.S. Capitol Police "may have suffered compromise in the cyber-attack."[91] USIS indicated this APT began in in late December 2013 and the last attacker activity was observed on July 4, 2014.[92] The USIS investigation also determined that this APT was focused on access to computer systems related to the background investigations business of USIS, which should have made it very clear to all stakeholders that the target was background investigation data.[93]

As a consequence of the USIS activity in the summer of 2014, US-CERT visited the facilities of KeyPoint Government Solutions (KeyPoint) to do a network assessment, which found items of concern that prompted additional review.[94] In December 2014, press reports indicated that KeyPoint had been breached resulting in the possible PII exposure of over 48,000 federal employees.[95] In June 2015, KeyPoint CEO Eric Hess testified before the Committee saying, "there was an individual who had an OPM account that happened to be a KeyPoint employee and that the credentials of that individual were compromised to gain access to OPM."[96] At the time of the 2015 data breach, OPM gave contractors a username and password and investigators would log-in with this OPM credential.[97]

In addition, OPM contractors holding sensitive healthcare information of federal employees have been the targets of APTs. In February 2015, Anthem, one of the largest health insurers in the country and provides coverage for 1.3 million federal employees, announced a data breach involving 80 million records of current and former customers and employees.[98] Then in March 2015, Premera, another health insurance company that has an OPM contract (covering about 130,000 federal workers in Washington state and Alaska), announced a data

[91] Letter from Counsel for U.S. Investigations Serv's, LLC (USIS) to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight & Gov't Reform at 5 (June 22, 2015).

[92] *Id.* at 5-6. In describing USIS activities related to the June 2014 discovery, USIS noted that an employee of the forensic investigation firm (Stroz Friedberg) they hired attempted to provide US-CERT additional forensic copies of hard drives with evidence of the attack on September 9, 2014, but the US-CERT employee declined saying "US-CERT [was] on a stand down." *Id.* Ex. 6.

[93] *Id.* at 6; *Id.* Ex. 12 Stroz Friedberg Summary of Investigation (Dec. 2014).

[94] *Hearing on OPM Data Breach: Part II* (statement of Ann Barron-DiCamillo, US-CERT Director).

[95] *See e.g.*, Christian Davenport, *KeyPoint Network Breach Could Affect Thousands of Federal Workers*, WASH. POST, Dec. 18, 2014, https://www.washingtonpost.com/business/economy/keypoint-suffers-network-breach-thousands-of-fed-workers-could-be-affected/2014/12/18/e6c7146c-86e1-11e4-a702-fa31ff4ae98e_story.html.

[96] *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, CEO KeyPoint Government Solutions); On June 29, 2015, the American Federation of Government Employees (AFGE) sued OPM over the data breach and also named KeyPoint as a defendant in the lawsuit.

[97] Saulsbury Tr. at 70-71. Wagner, the OPM Director of IT Security Operations said multiple credentials were compromised during the 2015 incident, but a KeyPoint credential was likely used for the initial attack vector. Wagner added "the adversary, utilizing a hosting server in California, created their own FIS [Federal Investigator Service, background] investigator laptop virtually. They built a virtual machine on the hosting server that mimicked and looked like a FIS investigator's laptop…and they utilized a compromise key point user credential to enter the network through the FIS contractor VPN portal." Wagner Tr. at 86, 128.

[98] Reed Abelson & Matthew Goldstein, *Millions of Anthem Customers Targeted in Cyberattack*, N.Y. TIMES, Feb. 5, 2015, available at: http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html?_r=0; Aliya Sternstein, *OPM Monitoring Anthem Hack; Feds Might be Affected* (Feb. 5, 2015) available at: http://www.nextgov.com/cybersecurity/2015/02/exclusive-opm-monitoring-anthem-hack-breach-could-impact-13m-feds/104700/.

breach that exposed medical data and financial information for 11 million customers.[99] These attacks highlight the persistent target that federal employee data presents and the need to secure such data – whether it is maintained in a federal or a contractor-operating IT system.

OPM, as well as other agencies, faces the challenge of securing their systems as well as overseeing the systems that government contractors operate on behalf of the government. In a 2014 report, GAO found that while agencies established security requirements and planned for assessments, the agencies reviewed (including OPM) failed to consistently oversee the execution and review of these assessments.[100] In response to GAO's recommendation to OPM "to develop, document and implement oversight procedures for ensuring that a system test is fully executed for each contractor-operator system," OPM promised to review "existing security policies and procedures" to enhance their oversight.[101] According to GAO's website, this recommendation remains open.[102]

In the case of the OPM background investigation contractors who experienced data breaches in 2014 and 2015, OPM had approved IT security plans for both USIS and KeyPoint.[103] In April 2015, GAO repeated the message about the need to address the cybersecurity challenge of ensuring effective oversight of contractors' implementation of security controls for systems contractors operate on behalf of agencies.[104] Based on testimony and documents submitted to the Committee, the record indicates that OPM had not informed USIS or KeyPoint about the March 2014 data breach before it became public.[105] It is unclear whether the attack could have been mitigated if OPM had informed their background investigation contractors, but given the threat environment and the background investigation systems targeted, it would have been prudent to alert the contractors – immediately.[106]

[99] *Premera Blue Cross Says Data Breach Exposed Medical Data* , N.Y. TIMES, Mar. 17, 2015, http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html; Elise Viebeck, *Federal Workers Might be Victims of Premera Data Breach*, THE HILL, Mar. 19, 2015, http://thehill.com/policy/cybersecurity/236266-federal-workers-might-be-victims-of-premera-breach.

[100] Gov't Accountability Office, GAO-14-612, *Agencies Need to Improve Oversight of Contractor Controls* (Aug. 2014), http://www.gao.gov/assets/670/665246.pdf.

[101] Gov't Accountability Office, GAO-14-612, *Agencies Need to Improve Oversight of Contractor Controls* 36 (Aug. 2014), http://www.gao.gov/assets/670/665246.pdf.

[102] *Open Recommendations for GAO-14-612, Agencies Need to Improve Oversight of Contractor Controls* GOV'T ACCOUNTABILITY OFFICE (last visited July 2, 2016), (http://www.gao.gov/recommendations/search?searched=1&hide_order_by_block=1&expand=&openrecs=&rows=10&now_sort=score+desc&page_name=main&q=GAO-14-612&field=rptno_ts

[103] *Hearing on OPM Data Breach: Part II* (testimony by Robert Giannetta, Chief Info. Officer, U.S. Investigations Services, LLC); Letter to the Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight and Gov't Reform from Counsel for U.S. Investigations Services, LLC (USIS) (June 22, 2015), Ex. 8, 9, 10 (ATOs signed by OPM and May 2014 OPM Site Survey Assessment Form); *Hearing on OPM Data Breach: Part II* (statement of Eric Hess, CEO KeyPoint Government Solutions); Email from KeyPoint Counsel to Majority Staff, H. Comm. on Oversight & Gov't Reform (Feb. 22, 2016) (on file with the Committee).

[104] *Enhancing Cybersecurity of Third Party Contractors and Vendors*: *Hearing Before H. Comm. on Oversight & Gov't Reform,* 114th Cong. (Apr. 22, 2015) (testimony of Gregory C. Wilshusen, Dir. Info. Sec. Issues, Gov't Accountability Office).

[105] *Hearing on OPM Data Breach: Part II* (statement of Robert Giannetta, Chief Info. Officer, U.S. Investigations Serv's, LLC). Despite a contractual obligation to notify contractors immediately of a "new or unanticipated threat or hazard," OPM did not notify their contractors (KeyPoint and USIS) of the March 2014 incident. *Id*

[106] *Hearing on OPM Data Breach: Part II* (Rep. Gowdy questioning of OPM contractors and OPM officials on the definition of "immediately.").

Agencies today rely on federal contractors to operate IT systems on behalf of the federal government and must access federal systems in order to perform services for the federal government. The potential risk of unauthorized access to IT systems operated by federal contractors on behalf of the federal government or contractors' IT systems should not have been surprising to OPM in the years leading up to the data breaches.

Federal Initiatives to Increase Information Security in Response to Increasing Attacks

As the first warnings of APT attacks began in 2005, the federal government was beginning to strengthen access controls. On August 5, 2005, OMB issued guidance to implement HSPD-12,[107] a Directive requiring the development and implementation of a mandatory, government-wide standard for secure and reliable forms of identification for federal employees and contractors. The guidance ("Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors") advised the heads of all departments and agencies that "[i]nconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risks to the Federal government."[108] The Administration issued HSPD-12 implementation guidance in the immediate years after the 2005 Directive was issued.[109]

In response to multiple attacks, in 2008, the federal government began a major new initiative to improve the security of its systems.[110] Meanwhile, attacks on federal systems continued and increased in volume and sophistication. Federal agencies only needed to look at attacks on government contractors and other private sector entities for a playbook about what they needed to able to counteract. In 2009, Chinese groups with ties to the People's Liberation Army reportedly carried out dozens of APT attacks against, *inter alia*, Northrop Grumman, Lockheed Martin, and Dow Chemical.[111]

[107] Memorandum from Joshua Bolton, Dir. Office of Mgmt. & Budget, Exec. Office of the President, to Dep't and Agency Heads, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 5, 2005). On August 27, 2004, the President signed HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive).

[108] Memorandum from Joshua Bolton, Dir. Office of Mgmt. & Budget, Exec. Office of the President, to Dep't and Agency Heads, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 5, 2005).

[109] Memorandum from Karen S. Evans, Admin'r, Office of E-Gov't & Info. Tech., Exec. Office of the President, to Chief Info. Officers, and Senior Agency Officials for Privacy, M-06-06, *Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12* (Feb. 17, 2006), https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-06.pdf. *See also* Exec. Office of the President, Press Release, *HSPD-12 Certified Products and Services Now Available for Agency Acquisition* (July 5, 2006), https://georgewbush-whitehouse.archives.gov/omb/pubpress/2006/2006-28.pdf.

[110] National Security Presidential Directive – 54 Cybersecurity Policy (Jan. 8, 2008) available at: https://fas.org/irp/offdocs/nspd/nspd-54.pdf.

[111] Fayyaz Rajpari, *Finding the Advanced Persistent Adversary*, SANS INST. (Sept. 29, 2014), https://www.sans.org/reading-room/whitepapers/hackers/finding-advanced-persistent-adversary-35512.

Four years later, the situation had not improved and appeared to be getting worse. A 2012 white paper by FireEye stated:

> Federal agencies are increasingly the victims of advanced persistent threats, often comprised of multi-staged, coordinated attacks that feature dynamic malware and targeted spear phishing emails. In fact, in spite of massive investments in IT security infrastructure, on a weekly basis, over 95% of organizations have at least 10 malicious infections bypass existing security mechanisms and enter the network. Further, 80% experience more than 100 new infections each week. Every day, mission-critical systems are compromised, and sensitive and classified data is exfiltrated from federal government and civilian networks.[112]

OPM itself was also targeted in the years leading up to the breaches discovered in 2014 and 2015. In May 2012, a hacker reportedly broke into an OPM database and stole 37 user IDs and passwords.[113] That breach was reportedly carried out by a group called "@k0detec," an activist affiliated with the hacking group Anonymous.[114] In 2011, the Department of Homeland Security issued a cybersecurity bulletin that called Anonymous "script kiddies" using "rudimentary" exploits. If true, Anonymous did not need advanced technical proficiency to gain access to an OPM database.[115]

OPM Failed to Recognize the Threat and Implement Effective IT Security Measures When It Mattered

The threat of APTs was well-known throughout the federal government and OPM was a prime target given the sensitive information it held on current and former federal employees and contractors. Thus, OPM should have made information security a top priority. In the years preceding the breaches at OPM in 2014 and 2015, however, information security was just one of several competing agency priorities, and network vulnerabilities became more acute. In late 2013 and early 2014, under Director Katherine Archuleta and CIO Donna Seymour, OPM attempted to re-focus on improving IT security. It did not work. Ineffective leadership and poor decision-making plagued the agency during a critical period in 2014, leaving the agency in a weak position to prevent the breaches.

[112] *Cyber Attacks on Government: How APT Attacks are Compromising Federal Agencies and How to Stop Them* FIREEYE (2012), http://www2.fireeye.com/rs/fireeye/images/fireeye-cyber-attacks-government.pdf.

[113] Paul Rosenzweig, *The Alarming Trend of Cybersecurity Breaches and Failures in the U.S. Government Continues*, HERITAGE FOUND. (Nov. 13, 2012), available at: http://www.heritage.org/research/reports/2012/11/cybersecurity-breaches-and-failures-in-the-us-government-continue (citing Privacy Rights Clearinghouse Chronology of Data Breaches available at: http://www.privacyrights.org/data-breach/new) ; *see also* Plaintiff's Class Action Complaint and Demand for Jury Trial, 21 (Aug. 14, 2015), Krippendorf v. U.S. Office of Personnel Mgmt., D.D.C. (No, 1:15 CV 01321) at 21 available at: http://blogs.reuters.com/alison-frankel/files/2015/08/krippendorfvopm-complaint.pdf

[114] Lee Johnstone, *U.S. Office of Personnel Management Hacked & Data Leaked by @k0detec*, CYBER WAR NEWS, May 23, 2012, available at: https://www.cyberwarnews.info/2012/05/23/u-s-office-of-personnel-management-hacked-data-leaked-by-k0detec/. That individual also carried out an attack on the Glade County Florida Sheriff's department

[115] Nat'l Cybersecurity & Comm'n Integration Ctr., Dep't of Homeland Sec., Bulletin A-0010-NCCIC - 160020110719.

OPM's Cybersecurity Spending Consistently Trailed Other Federal Agencies

OPM consistently reported spending less than other federal agencies on *cybersecurity*. In FY 2013, FY 2014 and FY 2015, OPM spent seven million each year on cybersecurity—spending that was consistently at the bottom relative to all other agencies that are required to report such expenditures to the Office of Management and Budget.[116] The previous fiscal year, 2012, OPM also lagged behind other federal agencies.

OPM sought additional funds for cybersecurity, but only after US-CERT notified the agency about the damaging breach in 2014. On March 20, 2014, OPM's Computer Incident Response Team (CIRT) received notification from DHS' US-CERT that data was being exfiltrated from OPM's network.[117] In the weeks that followed, OPM leadership would become aware the intrusion led to the breach of background investigation data in OPM systems holding the "crown jewels" of the American federal workforce and national security personnel.[118]

OPM requested additional cybersecurity funding in its FY 2016 Budget Justification (released February 2015), and only then (ten years after OPM took over the background investigation function) acknowledged it was a target rich environment. In a February 2, 2015 letter to the House Appropriations Subcommittee on Financial Services and General Government concerning its budget request, then-Director Katherine Archuleta noted: "OPM's FY2016 request is $32 million above our FY 2015 appropriation. Most of these funds will be directed towards investments in IT network infrastructure and security. As a proprietor of sensitive data—including personally identifiable information for 32 million federal employees and retirees—OPM has an obligation to maintain contemporary and robust cybersecurity controls."[119]

After years of neglect, the request for increased funding in February 2015 was too little too late. It came more than one year after attackers stole security documents that provided a roadmap to OPM's systems.[120] And the request came after hackers had already successfully exfiltrated sensitive data, including background investigations data in July and August of 2014 and federal employee personnel records in December 2014.[121]

[116] *See Infra*, Report Appendix: Cyber security Spending at OPM (Fiscal Years 2012-2015); *see also* Office of Mgmt. & Budget, Exec. Office of the President, *Annual Report to Congress: Federal Information Security Management Act* 82 (Mar. 18, 2016) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf. *See also* Office of Mgmt. & Budget, Exec. Office of the President, *Annual Report to Congress: Federal Information Security Management Act* 83 (Feb. 27, 2015) available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy14_fisma_report_02_27_2015.pdf.
[117] June 2014 OPM Incident Report at HOGR0818-001233.
[118] June 2014 OPM Incident Report at HOGR0818 -001245.
[119] U.S. Office of Pers. Mgmt., *OPM Congressional Budget Justification Performance Budget FY2016*, at 2 (Feb. 2015), https://www.opm.gov/about-us/budget-performance/budgets/congressional-budget-justification-fy2016.pdf.
[120] June 2014 OPM Incident Report, *at* HOGR0818 -001242.
[121] OPM Cybersecurity Events Timeline.

OPM Attempts to Balance IT Security with Competing Priorities

The year 2005 was a key year for both OPM and federal cybersecurity. The IG and US-CERT issued a general technical alert, which should have made OPM aware of the need to increase IT security in the face of increasing APT threats,[122] and OMB was gearing up to announce and begin implementation of HSPD-12.[123] The OPM IG also issued a warning in a semiannual report that would be repeated in subsequent reports. It warned:

> OPM relies on computer technologies and information systems to administer programs that distribute health and retirement benefits to millions of current and former federal employees and eligible family members. Any breakdowns or malicious attacks (e.g., hacking, worms or viruses) affecting these federal computer based programs could compromise efficiency and effectiveness and ultimately increase the cost to the American taxpayer.[124]

Amidst efforts to fortify federal cybersecurity, OPM was also working in 2005 to assume responsibility for the processing and storage of federal background investigations. OPM accepted the transfer of the Personnel Security Investigations function and personnel from the Department of Defense's Defense Security Service (DSS)—as authorized by the National Defense Authorization Act of 2004 (P.L. 108-136).[125] The transfer from DSS to OPM's Federal Investigative Services (FIS) division "brought under one roof a unit that is conducting 90 percent of background investigations for the entire Federal Government."[126]

Congress applied pressure on OPM to process the background investigation caseload more efficiently by tasking FIS with meeting timeframes imposed under The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458).[127] This was an important function in the wake of

[122] US-CERT, *Technical Cyber Security Alert TA05-189A: Targeted Trojan Email Attacks* (July 2005).

[123] Memorandum from Joshua Bolton, Dir. Office of Mgmt. & Budget, Exec. Office of the President, to Dep't and Agency Heads, M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 5, 2005). On August 27, 2004, the President signed HSPD-12 "Policy for a Common Identification Standard for Federal Employees and Contractors" (the Directive).

[124] Office of the Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2004 – March 31, 2005* 11 (May 1, 2005) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar32.pdf.

[125] U.S. Office of Pers. Mgmt., *FY2008 Congressional Budget Justification Performance Budget* 9 (Feb. 5, 2007) available at: https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf. U.S. Office of Pers. Mgmt., Press Release, *OPM Consolidates Bulk of Federal Security Clearance Process with Transfer of Over 1,800 Employees from Defense Department: Vast Majority of Federal Background Investigations to be Centered at OPM* (Nov. 22, 2004) ("The U.S. Office of Personnel Management and Department of Defense announced today the transfer of over 1,800 personnel security investigation staff from DoD to OPM. This move will consolidate the vast majority of background investigations for the Federal government with OPM.").

[126] U.S. Office of Pers. Mgmt., *FY2008 Congressional Budget Justification Performance Budget* 9 (Feb. 5, 2007) available at: https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf.

[127] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 50 U.S.C. § 3341(g) (2012); *see also* Rebeca Laflure, *How Congress Screwed Up America's Security Clearance System*, FOREIGN POLICY, Oct. 1, 2013 available at: http://foreignpolicy.com/2013/10/01/how-congress-screwed-up-americas-security-clearance-

the terrorist attacks in September 11, 2001. Various federal agencies and defense contractors increased their counter-terrorism staff.[128] That staffing surge caused a backlog in processing background investigations. The backlog was at least 188,000 by 2004.[129] The Intelligence Reform and Terrorism Prevention Act (P.L. 108-458) required that 90 percent of clearance applications had to be resolved within 60 days by 2009, a reduction of 84 percent from the then-375 day average wait time.[130]

Clearing the background investigation backlog was a priority, but there was also a clear need for OPM to prioritize the information security of its data. Over the 2005-2007 timeframe, the IG's annual auditing identified weaknesses in the security of the agency's information systems which would deteriorate to "material weakness" status in 2007.[131]

In March 2008, the IG's *Semiannual Report to Congress* recognized a need for the agency to focus on protecting sensitive information and PII over the long-term:[132]

> Unfortunately, in today's high tech world, inappropriate access to this sensitive information can lead to adverse consequences for the American public we are sworn to protect and serve. Consequently, the Office of the Inspector General (OIG) has identified and reported the protection of personally identifiable information as a top management challenge for the U.S. Office of Personnel Management (OPM), and we believe it is a challenge that will be ongoing because of the dynamic and ever-evolving nature of information security.
>
> Recognizing the adverse consequences of lost or stolen PII, including substantial harm, embarrassment and inconvenience to individuals, as well as potential identity theft, OPM's Director, the Honorable Linda M. Springer, initiated a series of actions beginning last fall. She wanted to make sure that all OPM employees clearly understood what PII meant, the importance of protecting PII, and their responsibilities in protecting it.[133]

system/; U.S. Office of Pers. Mgmt., *FY2008 Congressional Budget Justification Performance Budget* 9 (Feb. 5, 2007), https://www.opm.gov/about-us/budget-performance/budgets/2008-budget.pdf.

[128] *See, e.g.*, Rebeca Laflure, *How Congress Screwed Up America's Security Clearance System*, FOREIGN POLICY (Oct. 1, 2013) available at: http://foreignpolicy.com/2013/10/01/how-congress-screwed-up-americas-security-clearance-system/.

[129] *Id.*

[130] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 50 U.S.C. § 3341(g) (2012); *see also* Rebeca Laflure, *How Congress Screwed Up America's Security Clearance System*, FOREIGN POLICY, Oct. 1, 2013, http://foreignpolicy.com/2013/10/01/how-congress-screwed-up-americas-security-clearance-system/.

[131] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2007 – September 30, 2007,* at 10 (Sept. 2007) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar37.pdf.

[132] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2007 to March 31, 2008*, at i (Mar. 2008) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar38.pdf.

[133] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2007 to March 31, 2008*, at I (Mar. 2008) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar38.pdf. When the agency made a push in 2008 to ensure "all OPM employees clearly understand what PII meant, the importance of protecting PII, and their responsibilities in protecting it", OPM security staff that were

In the fall of 2008, however, the IG reported that the material weakness from the prior year had not been fully addressed, and that it had "some significant concerns" with aspects of the agency's information security program.[134] The IG warned that major elements of policies had not been updated in five years, found significant deficiencies existing in the control structure of OPM's management of major system certification and accreditation, as well as in the plan of action and milestones process, and that the agency operated without a permanent IT security officer for over six months.[135]

In the spring of 2009, OPM underwent a leadership transition. At John Berry's Senate confirmation hearing in March 2009, Mr. Berry was questioned extensively on the security clearance backlog,[136] however, Congress did not pose any questions to him about information security.[137]

Berry was confirmed in April 2009,[138] and in September 2009 he testified at length on the need to modernize the security clearance system and to eliminate the clearance backlog.[139] His prepared testimony noted that OPM's work to improve background investigation processing would include efforts to strengthen access controls. Berry testified:

> We are working to bring the benefits of access to the verification system to new user types to support agencies in Personal Identity Verification (PIV) credentialing. We are working with the stakeholder community to identify potential enhancement to the verification system to permit greater reciprocity. We are developing a web-based automated tool to assist agencies in identifying the appropriate level of investigation.[140]

Meanwhile in September 2009, the IG reported that the state of information security at OPM was worsening. The IG stated:

> In our FY 2007 and 2008 FISMA audit reports, we reported the lack of policies and procedures as a material weakness. While some progress was made in FY 2009, detailed guidance is still lacking. . . This year, we

key to the 2014 and 2015 breach response were already working at OPM. For example, Jeff Wagner, OPM's current Director of IT Security Operations, began working at OPM in June 2006. In transcribed interviews, Mr. Wagner also admitted that he had been on a Performance Improvement Plan (PIP) in 2012 or 2013. He said, "I believe the PIP that I was placed on was because, in my aggressive nature towards IT security, I had offended a few people." *See* Wagner Resume, at 000001 (OPM Production: Aug. 28, 2015); Wagner Tr. at 141-142.

[134] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2008 – September 30, 2008*, at 16 (2008) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar39.pdf.

[135] *Id.*

[136] *Nomination of Hon. M. John Berry to be Director, Office of Personnel Management: Hearing Before the S. Comm. on Homeland Sec. & Gov't Affairs,* 111th Cong. (Mar. 26, 2009).

[137] *Id.*

[138] U.S. Office of Pers. Mgmt., Press Release, *John Berry Confirmed as OPM Director* (Apr. 3, 2009) https://www.opm.gov/news/releases/2009/04/john-berry-confirmed-as-opm-director/.

[139] *Security Clearance Reform: Moving Forward on Modernization: Hearing Before the Subcomm. on Oversight of Gov't Mgmt, the Fed. Workforce, & D.C. of the S. Comm. On Homeland Sec. & Gov't Affairs*, 111th Cong. (Sept. 15, 2009) (statement of John Berry, Director, U.S. Office of Pers. Mgmt.).

[140] *Id.*

> expanded the material weakness to include the agency's overall information security governance program and included our concerns about the agency's information security management structure. For example, in the last 18 months, there has not been a permanent Senior Agency Information Security Official (SAISO) or a Privacy Program Manager, resulting in a serious decline in the quality of the agency's information security and privacy programs. With the recent appointment of the new SAISO, and the planned Office of Chief Information Officer reorganization which may involve increased staffing levels, we will reevaluate this issue during the FY 2010 FISMA audit.[141]

In the spring of 2010, the IG continued to report "significant concerns" regarding the overall quality of the information security program at OPM.[142] The IG warned that the agency had not fully documented information security policies and procedures or established appropriate roles and responsibilities, and that while an updated Information Security and Privacy Policy was finalized in August 2009, it did not specifically address OPM's IT environment and lacked detailed procedures and implementing guidance.[143] The IG also questioned in 2010 whether OPM leadership was committed to information security over the long-term. The IG stated:

> This year we expanded the material weakness to include the agency's overall information security governance program and incorporated our concerns about the agency's information security management structure. . . . The agency appointed a new SAISO in September 2009; however, the individual left in January 2010. Another new SAISO was appointed in late April 2010. With a new Chief Information Officer also recently selected, OPM may finally be in a position to make long needed improvements to its IT security program. However, given this turbulent history it remains to be seen whether senior management is fully committed to strong IT security governance for the long term."[144]

In 2012, OPM Director Berry ordered the centralization of IT security duties to a team within OPM's Office of Chief Information Officer (OCIO). In March 2012, the IG reported that "Our audit showed that the agency continues to struggle with improving the quality of its information security program."[145] The IG also found that the agency's OCIO lacked the authority it needed to manage security matters effectively, and that the agency needed to move to a more centralized system "because the fundamental design of the program is flawed."[146] The IG

[141] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress April 1, 2009 to September 30, 2009*, at 6-7 (Sept. 2009), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar41.pdf.

[142] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2009 – March 31*, 2010, at 7-8 (Mar. 2010), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar42.pdf.

[143] *Id.*

[144] *Id.*

[145] Office of Inspector Gen., U.S. Office of Pers. Mgmt., *Semiannual Report to Congress October 1, 2011 to March 31, 2012*, at 7 (Mar. 2012), https://www.opm.gov/news/reports-publications/semi-annual-reports/sar46.pdf.

[146] U.S. Office of Personnel Mgmt. Office of Inspector General *Semiannual Report to Congress October 1, 2012 to March 31, 2013*, at 8-9 (Mar. 2013) available at: https://www.opm.gov/news/reports-publications/semi-annual-reports/sar48.pdf.